# Building a Compliant Security Profile: ND TZI and NIST Certification for ERPUNO, COURT and COD security profiles

ERPUNO Security Team

14 червня 2026 р.

**Abstract**

This article details the methodology for constructing a Comprehensive Information Security System (KSZI) that complies with Ukrainian state standards (ND TZI) and the international NIST SP 800-53 framework. Using SYNRC/CA — an open source CMDB we demonstrate how to programmatically define, track, and audit a security profile. The approach utilizes Elixir-based Configuration Management Database (CMDB) profiles to maintain strict accountability over hardware, software, networks, data, roles, and risks. For security reasons we can only demo/showcase of ERPUNO security (sample) profile.

# Contents

# 1 Introduction

ERPUNO LLC provides high-tech telecommunication solutions for the automation of commercial and state enterprises. Their platform is architecturally divided into two primary layers:

- **Platform (SYS-APP-SYNRC):** The systemic foundation, including the Certificate Authority (CA), L2/L3 VPN tunnels, PKI-aware LDAP, Communicator (CHAT), BPMN process engine, MQTT broker, and KVS storage.
- **Products (SYS-APP-ERP):** Corporate and state enterprise systems such as Education (Edu), Healthcare (Health), Electronic Documents (Mail), Accounting (Acc), Warehouse Management, and Registries (Cart).

The company's architecture is built to support critical state and defense sector needs. It offers special licensing conditions for government applications, provided there is strict adherence to architectural compatibility and certification requirements (like DSSZZI). The system strictly follows ITU-T X-series, IETF RFC, NIST/FIPS, DSTU, and ISO/IEC standards (e.g., X.509, CMS/S-MIME, AES-GCM, Kyber, DSTU 4145-2002).

In this paper, we demonstrate how to build a unified security profile for this complex architecture. The CMDB system maps operational instances directly to NIST SP 800-53 controls (such as CM-8 for System Component Inventory, PM-5 for System Inventory) and ND TZI requirements (e.g., ND TZI 3.7-003-2023 for inventory and exploitation documentation).

## 1.1 Hierarchical Security Profiles (L1, L2, L3)

The system supports the automated construction of KSZI security profiles based on the regulatory and legal acts in the field of technical protection of information (TZI NPA). This automates documentation generation and the mapping of legislative requirements to technical settings. All certificates are issued with OID imprints of their respective security profiles.

The architecture is divided into three levels of profiles:

### 1.1.1 L1: Basic Security Profiles

These profiles define the fundamental sets of controls required by the regulations.

- **SECURITY POLICIES**[1]
- **FULL DIRECTORY (1123)**[2]
- **OPEN CONFIDENTIAL (126)**[3]

[1] `https://ca.n2o.dev/priv/security-profiles.pdf`
[2] `https://ca.n2o.dev/priv/bible_profile.pdf`
[3] `https://ca.n2o.dev/priv/legal_l1_profile_409.pdf`

- **OFFICIAL (155)**[4]

#### 1.1.2 L2: Industry Profiles

Industry-specific adaptations that expand upon the baseline controls to meet the requirements of specific sectors.

- **COURT INDUSTRY PROFILE**[5]: Industry security profile for the judicial system. It describes an extended set of baseline controls for processing sensitive information in state registries and courts, taking into account the requirements for high availability and data integrity based on ND TZI 3.6-006-24.
- **THE DIGITAL UKRAINIAN GOVERNMENT INDUSTRY PROFILE**[6]: Industry security profile for the Ministry of Digital Transformation of Ukraine.

#### 1.1.3 L3: Target Security Profiles

Specific implementation targets for individual systems and components.

- **ERP/1 SECURITY TARGET**[7]: Target profile for the ERP/1 telecommunications system. Describes the implementation of Attribute-Based Access Control (ABAC), information flow management (BPE), Public Key Infrastructure (PKI), and reliable auditing (KVS) for securing critical business processes.
- **X.509 CMS MESSAGING SECURITY TARGET**[8]: Target profile for corporate messenger systems. Based on X.509 and CMS (Cryptographic Message Syntax) cryptographic protocols, providing end-to-end encryption (E2EE), strict authentication, and non-repudiation for legally significant communications.
- **VPN SECURITY TARGET**[9]: Target profile for Virtual Private Network (VPN) and PKI infrastructures. Defines mechanisms for tunneling, node authentication (SC-8), and network traffic protection at the transport layer to secure communication channels against interception and modification.

### 1.2 Segregation of Duties: The Two-Stage KSZI Certification Process

According to the regulatory framework of Ukraine (e.g., ND TZI 2.6-001-11) and best global practices (the *Maker/Checker* principle), building and certifying

[4] `https://ca.n2o.dev/priv/legal_l1_profile_419.pdf`
[5] `https://ca.n2o.dev/priv/legal_l2_court_profile.pdf`
[6] `https://ca.n2o.dev/priv/digital-profile.pdf`
[7] `https://ca.n2o.dev/priv/legal_l3_profile_erp.pdf`
[8] `https://ca.n2o.dev/priv/chat_profile.pdf`
[9] `https://ca.n2o.dev/priv/vpn_profile.pdf`

a Comprehensive Information Security System (KSZI) is strictly a **two-stage procedure**. It requires the involvement of two completely independent licensed providers to eliminate any conflict of interest.

- **Stage 1: The Developer (Provider 1).** The first provider performs the risk assessment, inspects the environment, and creates the "technical instructions" — the **Target Security Profile (Technical Specification)**. This provider is also responsible for the physical implementation of the security architecture: configuring cryptography, setting up the Reference Monitor (AC-25), installing certificates, and delivering the system into trial operation.
- **Stage 2: The Expertise Organizer (Provider 2).** The second provider receives the Technical Specification from the Developer and designs the **Expertise Program**. This provider conducts an independent technical audit, instrumental testing, and live verification of all implemented controls. Upon successful verification, they issue the Expert Conclusion for the State Service of Special Communications and Information Protection (DSSZZI).

This segregation guarantees that the organization creating the security profiles and writing the Elixir CMDB structures is legally and practically distinct from the organization auditing and approving them.

## 1.3 The Three-Layer Security Profile Development Process

Constructing a comprehensive KSZI for ERP/1 follows a rigorous, sequential three-layer process. This sequence is not arbitrary — it mirrors the natural dependency chain of a security program: you must first organize your people and processes, then capture that organization into authoritative documentation and risk records, and only then implement the technical controls that enforce what the documentation prescribes.

1. **Layer 1 — Organizational Security Profile (Who and How).** The first layer establishes the human and procedural foundation. This includes defining roles and responsibilities (personnel security), establishing training and awareness programs, codifying incident response and maintenance procedures, and securing the physical environment. Without this layer, technical controls have no owner and no organizational context. `erpuno/itsm` and `zencrypted/ias` are the primary products that enforce this layer programmatically.
2. **Layer 2 — Metainformational Security Profile (What and Why).** The second layer translates the organizational decisions of Layer 1 into authoritative, machine-verifiable documentation: system security plans, risk taxonomies, data categorization matrices, privacy records, and acquisition

policies. The key innovation of ERP/1 is that this layer is not paper-based — it is expressed as live Elixir source code in the `synrc/ca` CMDB and automatically projected into audit-ready PDF reports. This eliminates documentation drift and guarantees that what auditors read is exactly what the system does.

3. **Layer 3 — Technical Security Profile (How Enforced).** The third layer implements the technical enforcement mechanisms that the first two layers define. Cryptographic access control, audit logging, network segmentation, integrity checking, and supply chain verification are all realized in specific ERP/1 products (`zencrypted/ias`, `erpuno/abac`, `synrc/vpn`, `synrc/kvs`, etc.). Technical controls reference and enforce the policies established in Layer 1 and documented in Layer 2.

This layered development model ensures full traceability: every technical control in Layer 3 can be traced back to a documented policy in Layer 2, which in turn traces back to an organizational decision in Layer 1. The entire chain is expressed in version-controlled source code, making the compliance posture continuously auditable and self-consistent.

# 2 Organizational Security Profile

The Organizational Security Profile establishes the human and procedural foundation of ERP/1 security. These controls define *who* is responsible for security, *how* they are trained, *how* incidents and maintenance are handled, *how* personnel are screened and off-boarded, and *how* the physical environment is protected. This layer must exist before the Metainformational layer can capture it in documentation, and before the Technical layer can enforce it in code.

The Organizational Security Profile covers the people, process, and physical environment controls of ERP/1. These are controls whose primary implementation vehicle is human procedure, training, and physical infrastructure, rather than software. The platform products in this section (`erpuno/itsm`, `zencrypted/ias`, `synrc/ca`) support and enforce these controls programmatically, but the controls themselves mandate organizational commitment.

## 2.1 Awareness and Training (AT)

### 2.1.1 `synrc/ca`: AT-2, AT-3 — Security Awareness and Role-Based Training

**AT-2 — Literacy Training and Awareness.** All ERP/1 users complete mandatory annual security awareness training covering phishing recognition, credential hygiene, incident reporting procedures, and acceptable use of cryptographic tokens. Completion is tracked via `zencrypted/ias`: the `training_completed_at` attribute must be current for the account to retain access. An expired training record triggers automatic account downgrade to read-only until training is renewed.

**AT-2(2) — Phishing Simulations.** `ias` integrates with the ERP/MAIL module to send automated simulated phishing campaigns quarterly. User responses (clicks, credential entry) are silently logged and bound to the user profile as a behavioral risk score attribute. High-risk users are automatically enrolled in remedial training and their sessions are subjected to enhanced monitoring by the SIEM.

**AT-3 — Role-Based Training.** `synrc/ca` provides a dedicated simulation environment (test HSM, test CA hierarchy) where security-critical roles — CA operators, HSM custodians, auditors — rehearse their procedures without impacting the production system. Key Ceremony rehearsals, OCSP failover drills, and CRL generation procedures are executed in this environment before being authorized for production.

## 2.2 Incident Response (IR)

### 2.2.1 `erpuno/itsm`: IR-1, IR-4, IR-5, IR-6

**IR-1 — Incident Response Policy and Procedures.** Incident response processes are formalized as BPMN processes in `synrc/bpmn` and executed via `erpuno/itsm`. Each incident type (with its MITRE ATT&CK code) has an

assigned BPMN template with clear stages: detection, classification, escalation, remediation, post-analysis.

**IR-4 — Incident Handling.** `itsm` automatically receives incidents from Wazuh (via webhook) and `ias` (upon detecting anomalies per AC-2(12)). Each incident receives a unique INC identifier, bound to the CMDB record of the affected component.

**IR-5 — Incident Monitoring.** The complete audit trail of each incident (all actions, comments, status changes) is stored in `kvs` and available for query. Retention period is a minimum of 3 years.

**IR-6 — Incident Reporting.** `itsm` automatically generates monthly incident reports in PDF format (using the `synrc/ca` LaTeX generator) and forwards them to the CISO and the relevant regulator (DSSZZI).

## 2.3 Maintenance (MA)

### 2.3.1 `erpuno/itsm`: MA-2, MA-4, MA-5

**MA-2 — Controlled Maintenance.** Any scheduled maintenance work (server, network equipment, HSM servicing) is registered as a Change Request (CR) in `itsm`. A CR has mandatory fields: `maintainer_id`, `authorization_certificate` (X.509 signature from an authorized engineer), `maintenance_window`, `rollback_plan`.

**MA-4 — Nonlocal Maintenance.** All remote maintenance access (SSH, RDP) is routed through a dedicated Jump server in the Management VLAN. Access to the Jump server is possible only from fixed IPs via an `synrc/vpn` tunnel with mandatory MFA.

**MA-5 — Maintenance Personnel.** The list of authorized maintenance personnel is maintained in the CMDB (`roles.ex`) and verified by `ias` before granting access. Non-certified personnel are technically unable to access the systems.

## 2.4 Personnel Security (PS)

### 2.4.1 `zencrypted/ias`: PS-3, PS-4, PS-5, PS-6, PS-7 — Personnel Lifecycle

**PS-3 — Personnel Screening.** Background verification requirements for each role are encoded as mandatory attributes in `ias` account profiles. An account with role `security_admin` or `global_root_admin` cannot be activated without the `background_check_completed` attribute set by an authorized HR officer. This creates a technical enforcement of the screening policy.

**PS-4 — Personnel Termination.** When an employee termination event is received from the HR module (via SCIM 2.0 or webhook), `ias` executes a deterministic off-boarding sequence within one minute: (1) all active sessions are revoked, (2) the account is suspended, (3) all X.509 certificates are submitted for OCSP revocation to `synrc/ca`, (4) group memberships are removed, and (5) a termination audit event is written to `kvs`. This eliminates the risk of access persisting after termination.

**PS-5 — Personnel Transfer.** Role transfers are handled via the Joiner-Mover-Leaver (JML) workflow in `erpuno/itsm`. A transfer Change Request must be approved by both the origin and destination supervisors. Upon approval, `ias` simultaneously removes old role attributes and adds new ones, then requests issuance of a new X.509 certificate reflecting the updated role set from `synrc/ca`.

**PS-6 — Access Agreements.** As described in PL-4, access agreements (rules of behavior) are accepted cryptographically during certificate enrollment. The signed enrollment request itself constitutes the access agreement. Changes to the rules of behavior trigger a new certificate enrollment cycle, requiring fresh cryptographic acceptance.

**PS-7 — External Personnel Security.** Third-party contractors and external auditors receive time-limited X.509 certificates from a dedicated sub-CA with a restricted OID scope in `synrc/ca`. These certificates have a hard expiration aligned with the contract period, after which access terminates automatically without any manual action. The ABAC policies for the `external_contractor` role enforce a strict Default Deny posture, granting only explicitly scoped resource access.

## 2.5 Physical and Environmental Protection (PE)

### 2.5.1 `synrc/ca` CMDB: PE-2, PE-3, PE-6, PE-12 — Physical Access and Environment

**PE-2 — Physical Access Authorizations.** Physical access to the server room and HSM storage area is controlled via a PKI-based electronic access control system. The authorized persons list is maintained as a CMDB record (`hw.ex` physical zone policy), cross-referenced with active `ias` accounts. A deactivated account automatically triggers removal from the physical access list within one synchronization cycle.

**PE-3 — Physical Access Control.** The server room enforces a mantrap entry with dual authentication: PKI smart card (verified against `synrc/ca` OCSP) plus biometric. The HSM area additionally requires dual-person integrity (two authorized persons must enter together) — a physical enforcement of the Dual Control principle mandated for all cryptographic key operations.

**PE-6 — Monitoring Physical Access.** CCTV feeds from all access points are retained for 90 days. Motion events and access log entries are correlated by Wazuh: an access event without a corresponding `ias` login event (or vice versa) generates an anomaly alert, detecting tailgating, piggybacking, or account sharing.

**PE-12 — Emergency Lighting.** The data center is equipped with UPS (HPE R/T3000) and diesel generator backup power, documented in `hw.ex` as `ERP-PE-UPS-01` and `ERP-PE-GEN-01`. Emergency lighting and environmental monitoring (temperature, humidity, fire suppression status) feed into Zabbix, with threshold alerts routed to the on-call infrastructure team via `erpuno/itsm`.

# 3 Metainformational Security Profile

The Metainformational Security Profile translates the organizational decisions established in Layer 1 into authoritative, machine-verifiable governance artifacts. Rather than static paper documents, ERP/1 expresses all security plans, risk taxonomies, data categorizations, and privacy records as live, version-controlled Elixir source code within `synrc/ca`. These artifacts are the formal bridge between organizational intent and technical enforcement: technical controls in Layer 3 enforce exactly what this layer documents, and this layer documents exactly what Layer 1 mandates.

The Metainformational Security Profile covers the governance, planning, and programmatic documentation layer of ERP/1. These controls are realized through the CMDB paradigm: instead of static paper artifacts, all policy and risk information is expressed as live, version-controlled Elixir source code in `synrc/ca`. This makes the security documentation self-verifying, continuously synchronized with the deployed system, and automatically auditable by state regulators (DSSZZI) and international auditors (ISO/IEC 27001, NIST).

## 3.1 Planning (PL)

### 3.1.1 `synrc/ca`: PL-2, PL-4, PL-8 — System Security Plans and Rules of Behavior

**PL-2 — System Security and Privacy Plans.** The system security plan for ERP/1 is not a Word document filed in a binder. It is this very PDF report, generated on demand via `mix run -e 'CA.TeX.gen_bible()'` from the live CMDB state. Every section — hardware inventory, risk taxonomy, role definitions, network architecture — is extracted programmatically, ensuring 100% fidelity between documentation and deployed reality. The plan is updated automatically upon every git commit that changes a CMDB module.

**PL-4 — Rules of Behavior.** Acceptable use rules are defined declaratively in `roles.ex` and embedded as machine-readable OID extensions in X.509 certificates. Every certificate holder cryptographically acknowledges the rules of behavior by accepting and installing their certificate, creating an auditable, non-repudiable consent record stored in `kvs`.

**PL-8 — Security and Privacy Architectures.** The security architecture of ERP/1 is codified as the L3 Target Security Profile (`legal_l3_profile_erp.pdf`), generated from CMDB and cryptographically signed. Any deviation from the declared architecture is detectable by comparing the current CMDB state against the signed baseline, enabling automated drift detection.

## 3.2 Program Management (PM)

### 3.2.1 `synrc/ca` CMDB: PM-2, PM-5, PM-6, PM-9 — Security Program Infrastructure

**PM-2 — Information Security Program Leadership Roles.** The CMDB `roles.ex` module formally defines the organizational security roles: Security Administrator (`security_admin`), Auditor (`auditor`), Registration Operator (`reg_operator`), and Global Superadministrator (`global_root_admin`). These roles are not notional — they are enforced cryptographically via X.509 certificate extensions and ABAC policies.

**PM-5 — System Inventory.** `CA.PRO.inventory/1` delivers a real-time, programmatically queryable hardware inventory (`hw.ex`), satisfying PM-5 in a machine-verifiable form. The inventory is linked to cryptographic certificates, so any undocumented asset lacks a valid mTLS credential and is automatically rejected by the platform.

**PM-6 — Measures of Performance.** Security performance metrics (control coverage ratios, incident counts, certificate expiration timelines) are extracted via `CA.PRO` queries and embedded in automatically generated PDF reports. This eliminates manual metric collection and guarantees that reported figures reflect the actual system state at the moment of report generation.

**PM-9 — Risk Management Strategy.** The organizational risk management strategy is materialized in `risk.ex` — a structured registry of over 40 threat scenarios (RISK-OS-01 through RISK-DAT-02), each tagged to specific NIST control families. This ensures that every identified risk has a corresponding mapped control, and every unmapped risk generates a POA&M entry tracked in `erpuno/itsm`.

## 3.3 Risk Assessment (RA)

### 3.3.1 `synrc/ca` risk.ex: RA-2, RA-3, RA-5 — Programmatic Risk Taxonomy

**RA-2 — Security Categorization.** Data categorization for ERP/1 (Public, PII, Internal, Confidential) is encoded in `data.ex`. Each category is automatically coupled to mandatory cryptographic and access control requirements: PII data triggers PostgreSQL TDE + ABAC restrictions; Confidential data mandates HSM-backed encryption and air-gapped backup routing. Categorization is machine-enforced, not advisory.

**RA-3 — Risk Assessment.** The `risk.ex` module maintains a living threat model. Risks are classified by attack vector (OS, Crypto, Network, Infrastructure, Personnel, Synchronization, Data) and mapped to specific NIST control families. The taxonomy is re-evaluated on every system change: when a new hardware component appears in `hw.ex`, the risk engine automatically checks for unmitigated threats applicable to that component class.

**RA-5 — Vulnerability Monitoring and Scanning.** Vulnerability data from the `risk.ex` taxonomy is cross-referenced against the Wazuh SIEM feed

and automated SBOM dependency scans in the CI/CD pipeline. Any newly disclosed CVE matching a component in `sys.ex` triggers an automatic risk record update and incident creation in `erpuno/itsm`.

## 3.4 System and Services Acquisition (SA)

### 3.4.1 `synrc/ca` + CI/CD: SA-5, SA-9, SA-11 — Documentation as Code and Vendor Security

**SA-5 — System Documentation.** The cornerstone of the ERP/1 metainformational approach is the "Documentation as Code" (DaC) paradigm. The entire KSZI documentation package — security plans, asset registries, risk matrices, network diagrams, this PDF — is generated from live Elixir source code. The command `mix run` produces a complete, audit-ready documentation set. Documentation is never manually edited; it is always a faithful projection of the code state.

**SA-9 — External System Services.** All external services used by ERP/1 (TSA providers for RFC 3161, OCSP endpoints, external IdP federation) are formally declared in `sys.ex` CMDB with their security classification, interface type, and contractual agreements. Undeclared external dependencies are blocked at the mTLS boundary, since they cannot possess a certificate issued by `synrc/ca`.

**SA-11 — Developer Testing and Evaluation.** All ERP/1 components undergo automated security testing at the CI/CD pipeline level: SBOM generation, OWASP Dependency Check, static analysis (Credo), and cryptographic signature verification before any artifact reaches the production registry. Test results are stored as CMDB events and are queryable by auditors.

## 3.5 Privacy (PT)

### 3.5.1 `synrc/ca` CPS: PT-2, PT-4, PT-6 — Authority, Consent, and PII Accuracy

**PT-2 — Authority to Process Personally Identifiable Information.** The legal basis and specific purposes for processing personal data (subscriber registry: passport data, RNOKPP) are declared in the Certificate Practice Statement (CPS), published at `https://ca.n2o.dev`. The CPS is a legally binding document, version-controlled in Git, and referenced by OID in every issued certificate.

**PT-4 — Consent Management.** Every subscriber provides a digitally signed consent form (XAdES-BES) during the registration process. This consent is stored in `kvs` as an immutable event, preserving the exact scope of consent accepted, the version of the CPS in force at the time, and the timestamp (RFC 3161). This provides legally valid evidence of informed consent for the entire duration of the certificate's validity.

**PT-6 — Disassociation.** Upon subscriber request or legal obligation, personal data is pseudonymized or erased from the active database. The immutable audit log in `kvs` retains only the cryptographic hash of the erased record and the

legal basis for the erasure, satisfying both the right to erasure and the obligation to maintain an audit trail of security-relevant events.

## 3.6 Security Evaluation Framework

The following sections provide the complete execution traces of the CMDB profile extraction for the "ERP" system. These outputs demonstrate how the infrastructure is documented, maintained, and continuously monitored.

### 3.6.1 Risk Assessment (CA.PRO.risk)

The risk taxonomy enumerates the identified threats and binds them to the corresponding security control families.

```
iex> CA.PRO.risk("ERP")
[
  {"RISK-OS-01", "Вразливості Active Directory (Kerberoasting, Pass-the-Hash, Golden Ticket)", ["AC", "IA", "SC"]},
  {"RISK-OS-02", "Зловживання WMI та PowerShell (Fileless-методи)", ["SI", "SC", "CM"]},
  {"RISK-OS-03", "Вразливості на рівні ядра (BYOVD, Ring 0)", ["SI", "CM"]},
  {"RISK-OS-04", "Маніпуляція маркерами доступу (Token Stealing)", ["AC", "AU"]},
  {"RISK-OS-05", "Некоректні дозволи NTFS / Share (Orphaned SIDs)", ["AC", "CM"]},
  {"RISK-OS-06", "Підвищення привілеїв Linux (Kernel, SUID, Dirty COW)", ["AC", "SI"]},
  {"RISK-OS-07", "Втеча з контейнерів Docker/Kubernetes", ["SC", "CM"]},
  {"RISK-OS-08", "Зловживання eBPF (прихований моніторинг)", ["AU", "SI"]},
  {"RISK-OS-09", "Ін'єкції динамічних бібліотек (LD_PRELOAD)", ["SI", "CM"]},
  {"RISK-OS-10", "Вразливості PAM (обхід автентифікації)", ["IA", "AC"]},
  {"RISK-OS-11", "Обхід XProtect / Gatekeeper / SIP (macOS)", ["CM", "SI"]},
  {"RISK-OS-12", "Компрометація macOS Keychain", ["IA", "SC"]},
  {"RISK-OS-13", "TCC Bypass & Spyware (macOS)", ["SI", "PE"]},
  {"RISK-OS-14", "Dyld Hijacking (macOS)", ["SI"]},
  {"RISK-OS-15", "Обхід Pointer Authentication PAC (Apple Silicon)", ["SI", "SA"]},
  {"RISK-CRY-01", "Пост-квантові загрози SNDL (Store Now, Decrypt Later)", ["SC", "RA", "SA"]},
  {"RISK-CRY-02", "Атаки сторонніми каналами (DPA, таймінг, EM)", ["SC", "PE", "SA"]},
  {"RISK-CRY-03", "Fault Injection (Glitching, Voltage Drop)", ["PE", "SI", "SC"]},
  {"RISK-CRY-04", "Компрометація ПАК «Гряда» (IIT HSM)", ["PE", "SC", "AC"]},
  {"RISK-CRY-05", "Екстракція ключів з НКІ е-Токен (IIT)", ["PE", "SC"]},
  {"RISK-CRY-06", "Вразливості ASN.1 парсерів X.509 / CMS", ["SI", "SA"]},
  {"RISK-CRY-07", "Вразливості криптобібліотек ДСТУ (Калина, Купина, Padding Oracle)", ["SA", "SI"]},
  {"RISK-CRY-08", "Недостатня ентропія генератора псевдовипадкових чисел (PRNG)", ["SC"]},
  {"RISK-CRY-09", "Втрата або перехоплення PIN-кодів HSM (кейлогери)", ["IA", "AT", "PE"]},
  {"RISK-CRY-10", "Фізична деструкція носіїв «Автор» (CryptoCard)", ["PE", "MP"]},
  {"RISK-CRY-11", "Вразливості CCID драйверів токенів (ескалація привілеїв)", ["SI", "CM"]},
  {"RISK-CRY-12", "Підміна сесій PKCS#11 (MitM між ПЗ ЦСК та HSM)", ["SC", "SI"]},
  {"RISK-NET-01", "BGP Hijacking & Route Leaks (підміна анонсів AS)", ["SC", "SI"]},
  {"RISK-NET-02", "Атаки L2 (VLAN Hopping, ARP Spoofing, STP атаки)", ["SC", "AC"]},
  {"RISK-NET-03", "Вразливості IPSec / VPN (IKE downgrade, PSK витік)", ["SC", "IA"]},
  {"RISK-NET-04", "DDoS (Slowloris, SYN Flood, ампліфікація DNS/NTP)", ["SC", "IR"]},
  {"RISK-NET-05", "Компрометація Wi-Fi (KRACK, PMKID, Evil Twin)", ["SC", "IA"]},
  {"RISK-NET-06", "Вразливості DNSSEC (DNS Spoofing, помилки конфігурації)", ["SC", "SI"]},
  {"RISK-NET-07", "Відкриті інтерфейси управління (SNMPv1/v2, Telnet, REST API)", ["CM", "AC", "SC"]},
  {"RISK-INF-01", "Компрометація BMC (IPMI, iDRAC, iLO)", ["AC", "SC"]},
  {"RISK-INF-02", "Вразливості Firmware / UEFI Bootkits", ["SI", "SA"]},
  {"RISK-INF-03", "Атаки на мікроархітектуру CPU (Spectre, Meltdown)", ["SI", "SC"]},
  {"RISK-INF-04", "Cold Boot & Rowhammer атаки на пам'ять", ["PE", "SI"]},
  {"RISK-INF-05", "Відмова дискових масивів SAN/NAS (Split-brain)", ["CP", "SI"]},
  {"RISK-INF-06", "Електромагнітне випромінювання TEMPEST", ["PE", "SC"]},
  {"RISK-INF-07", "Відмова інженерних систем (UPS, дизель, чиллер, пожежогасіння)", ["PE", "CP"]},
  {"RISK-PER-01", "Spear Phishing & Whaling (цільовий фішинг адміністраторів)", ["AT", "IR", "SI"]},
  {"RISK-PER-02", "Watering Hole Attacks (компрометація профільних ресурсів)", ["SI", "AT"]},
  {"RISK-PER-03", "Інсайдерський саботаж та ексфільтрація (логічні бомби)", ["PS", "AU", "AC"]},
  {"RISK-PER-04", "Pretexting / Baiting / Tailgating (фізичний доступ)", ["AT", "PE", "PS"]},
  {"RISK-PER-05", "Credential Stuffing (словники та бази паролів)", ["IA", "AT"]},
  {"RISK-SYNC-01", "Race Condition (стан гонитви у спільних ресурсах)", ["SI", "SA"]},
  {"RISK-SYNC-02", "TOCTOU (Time-of-Check to Time-of-Use)", ["SI", "AC"]},
  {"RISK-SYNC-03", "NTP Spoofing (десинхронізація часу)", ["SC", "AU", "SI"]},
  {"RISK-SYNC-04", "Split-Brain у кластерах СУБД", ["CP", "SI"]},
  {"RISK-SYNC-05", "Replication Lag (вікно доступу до застарілих даних)", ["SI", "SC"]},
  {"RISK-DAT-01", "Втрата резервних копій (Ransomware, Backup Corruption)", ["CP", "MP", "SI"]},
```

```
  {"RISK-DAT-02", "Витік електронних судових справ (несанкціонований доступ)", ["AC", "SC", "PE"]}
]
```

### 3.6.2 System Software Components (CA.PRO.sys)

The system inventory documents all OS, middleware, platform, and application-level software components running in the environment, satisfying NIST CM-8 and PM-5.

```
iex> CA.PRO.sys("ERP")
[
  {"SYS-OS-01-UAL", "UA Linux 24.04 LTS (ДСТУ-hardened, SELINUX Enforcing) (24.04 LTS)", []},
  {"SYS-OS-01-WIN", "Windows Server 2025 Datacenter (NATO STIG + DISA hardened) (2025 Datacenter)", []},
  {"SYS-OS-01-ESX", "VMware ESXi 8.0 Update 3 (vSphere Foundation) (8.0 U3)", []},
  {"SYS-OS-02-W11", "Windows 11 Pro 24H2 (DISA STIG + Windows Defender Credential Guard) (24H2 (Build 26100))", []},
  {"SYS-OS-02-UAL", "UA Linux Desktop 24.04 LTS (ДСТУ, GNOME Hardened) (24.04 LTS Desktop)", []},
  {"SYS-APP-00-ERL", "Erlang/OTP 27.3 (SMP, BEAM VM, distribution TLS) (27.3)", []},
  {"SYS-APP-00-ELX", "Elixir 1.18.3 (N2O, NITRO, FORM, Bandit) (1.18.3)", []},
  {"SYS-APP-00-EMQ", "EMQ X 2.12 (MQTT 5.0 / MQTT-SN, Erlang/OTP cluster) (2.12)", []},
  {"SYS-SYNRC-CA", "Сертифікати (7.4)", []},
  {"SYS-SYNRC-VPN", "Тунелі (1.0)", []},
  {"SYS-SYNRC-LDAP", "Директорія (1.0)", []},
  {"SYS-SYNRC-CHAT", "Комунікатор (4.2)", []},
  {"SYS-SYNRC-BPMN", "Процеси (6.11)", []},
  {"SYS-SYNRC-MQTT", "Брокер (2.12)", []},
  {"SYS-SYNRC-KVS", "Сховище (10.0)", []},
  {"SYS-SYNRC-WS", "Фреймворк (11.0)", []},
  {"SYS-SYNRC-FORM", "Форми (1.3)", []},
  {"SYS-SYNRC-ASN1", "Компілятор (1.0)", []},
  {"SYS-SYNRC-ABAC", "Контроль (1.0)", []},
  {"SYS-ERP-EDU", "Освіта (1.0)", []},
  {"SYS-ERP-HEALTH", "Здоров'я (1.0)", []},
  {"SYS-ERP-MAIL", "Документи (1.0)", []},
  {"SYS-ERP-ACC", "Облік (1.0)", []},
  {"SYS-ERP-WAREHOUSE", "Склад (1.0)", []},
  {"SYS-ERP-CART", "Реєстри (1.0)", []},
  {"SYS-APP-01-IIT", "IIT Користувач ЦСК-1 (бібліотека «IIT Gryada-301») (3.0.1)", []},
  {"SYS-APP-01-CIP", "Сайфер HSM Middleware (PKCS#11 + CMS + TSP клієнт) (2.8)", []},
  {"SYS-APP-01-SIGN", "Автор Е-Підпис Сервер (batch signing, LTV, XAdES-BES) (5.2)", []},
  {"SYS-APP-02-WZ", "Wazuh 4.9 SIEM/XDR (OSSEC-based, FIM, compliance CIS/NIST) (4.9)", []},
  {"SYS-APP-02-ZBX", "Zabbix 7.2 (active agents, encrypted PSK transport, alerting) (7.2 LTS)", []},
  {"SYS-DB-01-PG", "PostgreSQL 17.2 (TDE + pgAudit + pg_partman) (17.2)", []},
  {"SYS-DB-01-ORA", "Oracle Database 23ai (Advanced Security Option, TDE, Vault) (23ai (23.5))", []},
  {"SYS-DB-02-RDS", "Redis 7.4 (TLS 1.3, ACL, persistence RDB+AOF) (7.4)", []},
  {"SYS-INF-01-VBR", "Veeam Backup & Replication 12.3 (immutable backups, SureBackup) (12.3)", []},
  {"SYS-INF-01-BCL", "Bacula Community 15.0 (offline tape + air-gapped archive) (15.0)", []},
  {"SYS-MW-01-NGX", "Nginx 1.27 (TLS 1.3 only, OCSP Stapling, CT Logs, HSTS) (1.27)", []},
  {"SYS-MW-01-HAP", "HAProxy 3.0 (HA pair, health checks, rate limiting) (3.0 LTS)", []},
  {"SYS-MW-02-AD", "Active Directory Domain Services 2025 (LAPS v2, Protected Users, Tiering) (Windows Server 2...", []},
  {"SYS-MW-02-IPA", "FreeIPA 4.12 (Kerberos V, OTP, CA sub-ідентифікатор) (4.12)", []}
]
```

### 3.6.3 Hardware Inventory (CA.PRO.inventory)

The hardware inventory explicitly tracks physical assets, cryptographic modules (HSMs), network appliances, and storage arrays.

```
iex> CA.PRO.inventory("ERP")
[
  {"ERP-STG-01", "ERP-STG-2025-001", "5HT Technology AllFlash NVMe Array (Sapphire Rapids Storage Controller)"},
  {"ERP-STG-02", "ERP-STG-2025-002", "5HT Technology AllFlash NVMe Array"},
  {"ERP-TAPE-01", "ERP-STG-2025-003", "HPE StoreEver MSL3040 Tape Library"},
  {"ERP-WS-01", "ERP-WS-2025-001", "5HT Technology Workstation Compact (Sapphire Rapids)"},
```

```
  {"ERP-WS-02", "ERP-WS-2025-002", "5HT Technology Workstation Compact (Sapphire Rapids)"},
  {"ERP-KZI-01", "ERP-KZI-2025-001", "IIT Gryada-301 PCIe HSM"},
  {"ERP-KZI-02", "ERP-KZI-2025-002", "IIT Gryada-301 PCIe HSM"},
  {"ERP-KZI-03", "ERP-KZI-2025-003", "Автор CryptoCard Smart-01 (e-Токен, Смарт-карта)"},
  {"ERP-NET-01", "ERP-NET-2025-001", "Cisco Catalyst 9500-48Y4C"},
  {"ERP-NET-02", "ERP-NET-2025-002", "Cisco Catalyst 9500-48Y4C"},
  {"ERP-NET-03", "ERP-NET-2025-003", "Cisco ASR 1002-HX Router"},
  {"ERP-FW-01", "ERP-NET-2025-004", "Cisco Firepower 4145 NGFW (FTD 7.6)"},
  {"ERP-FW-02", "ERP-NET-2025-005", "Cisco Firepower 4145 NGFW (FTD 7.6)"},
  {"ERP-SRV-01", "ERP-2025-001", "5HT Technology Tristellar 3U"},
  {"ERP-SRV-02", "ERP-2025-002", "5HT Technology Tristellar 3U"},
  {"ERP-SRV-03", "ERP-2025-003", "5HT Technology Quadstellar 4U"},
  {"ERP-SRV-04", "ERP-2025-004", "5HT Technology Quadstellar 4U"},
  {"ERP-SRV-05", "ERP-2025-005", "5HT Technology Tristellar 3U"},
  {"ERP-SRV-06", "ERP-2025-006", "5HT Technology Tristellar 3U"},
  {"ERP-SRV-07", "ERP-2025-007", "5HT Technology Tristellar 3U"},
  {"ERP-SRV-08", "ERP-2025-008", "5HT Technology Tristellar 3U"}
]
```

### 3.6.4 Role-Based Access Control (CA.PRO.roles)

The defined roles establish the baseline for the Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) mechanisms.

```
iex> CA.PRO.roles("ERP")
[
  {"ROLE-ADM-01", "Адміністратор безпеки", ["security_admin"]},
  {"ROLE-AUD-01", "Аудитор", ["auditor"]},
  {"ROLE-OPR-01", "Оператор реєстрації", ["reg_operator"]},
  {"ROLE-SYS-01", "Системний процес (Machine-to-Machine)", ["ocsp_service", "crl_generator"]},
  {"ROLE-SADM-01", "Глобальний суперадміністратор (root/administrator)", ["global_root_admin", "infra_super_user"]}
]
```

### 3.6.5 Data Categorization (CA.PRO.data)

Data categorization ensures that sensitive information (e.g., PII, keys) is stored in the appropriate encypted and access-controlled repositories.

```
iex> CA.PRO.data("ERP")
[
  {"DATA-PUB-01", "Публічні сертифікати та CRL", "Public CDN / web server"},
  {"DATA-PUB-02", "Політики ЦСК (CPS, CP)", "Public web server"},
  {"DATA-PII-01", "Реєстр підписників (паспорти, РНОКПП)", "Encrypted DB (PostgreSQL)"},
  {"DATA-PII-02", "Адресні та контактні дані підписників", "Encrypted DB (PostgreSQL)"},
  {"DATA-INT-01", "Внутрішні накази та регламенти", "Internal file server"},
  {"DATA-INT-02", "Журнали аудиту (SIEM logs)", "SIEM (Elasticsearch)"},
  {"DATA-KEY-01", "Кореневі та підпорядковані ключі ЦСК", "HSM (Гряда / IIT)"},
  {"DATA-KEY-02", "Паролі та секрети адміністраторів", "Password Manager (Vault)"},
  {"DATA-CRT-01", "Матеріали судових проваджень та ухвали", "Encrypted DB (Oracle / PostgreSQL)"},
  {"DATA-CRT-02", "Електронні докази (обмежений доступ)", "Encrypted storage (Scality RING)"},
  {"DATA-BKP-01", "Снапшоти БД та образи ВМ", "Tape Library (MSL3040)"},
  {"DATA-BKP-02", "Офлайн-архіви судових документів", "Air-gapped Tape (offline)"}
]
```

### 3.6.6 Business Processes (CA.PRO.proc)

The documentation of business processes connects operational workflows with their responsible actors, ensuring accountability.

```
iex> CA.PRO.proc("ERP")
[
  {"PROC-CERT-01", "Видача кваліфікованих сертифікатів", "Оператор реєстрації ЦСК"},
  {"PROC-OCSP-01", "Формування OCSP-відповідей (24/7)", "Автоматичний сервіс ЦСК"},
  {"PROC-AUDIT-01", "Логування та моніторинг подій безпеки", "Адміністратор безпеки / SIEM"},
  {"PROC-ROOT-01", "Церемонія генерації кореневого ключа", "Комісія ЦСК (Dual Control)"},
  {"PROC-DOC-01", "Реєстрація та розгляд судових справ", "Судова влада України / ДП ІСС"},
  {"PROC-BKP-01", "Резервне копіювання та відновлення", "Адміністратор резервного копіювання"}
]
```

### 3.6.7 Network Architecture (CA.PRO.net)

The network segmentation profile details the logical separation of DMZ, internal, management, and air-gapped zones to prevent lateral movement.

```
iex> CA.PRO.net("ERP")
[
  {"NET-DMZ-01", "OCSP / CRL публічний ендпоінт", "публічна підмережа"},
  {"NET-DMZ-02", "Веб-портал ЦСК", "публічна підмережа"},
  {"NET-INT-01", "Сегмент серверів БД", "внутрішня підмережа БД"},
  {"NET-INT-02", "Сегмент робочих станцій операторів", "внутрішня підмережа АРМ"},
  {"NET-MGT-01", "VLAN IPMI / iLO адміністрування", "management VLAN"},
  {"NET-AIR-01", "Кореневий ЦСК (офлайн вузол)", "N/A"}
]
```

# 4 Technical Security Profile

The Technical Security Profile implements the enforcement mechanisms that the organizational procedures of Layer 1 mandate and the governance documentation of Layer 2 describes. Every control in this section is traceable: `AC-2` enforces the personnel lifecycle defined in PS-4 and documented in PM-2; `AU-12` enforces the audit event catalog defined in AU-2 policy and encoded in the CMDB. The ERP/1 architecture ensures that no technical control exists without organizational ownership, and no organizational policy exists without technical enforcement.

The following section is a comprehensive, control-by-control scientific analysis of how the components of the ERP/1 platform (ecosystem `ERP.UNO`, `N2O.DEV`, `SYNRC.COM`) naturally and architecturally satisfy the requirements of NIST SP 800-53 Rev.5 and ND TZI 2.3-025-24. Each platform product is a purpose-built solution for a specific security domain, enabling maximally organic — without artificial mappings — standard compliance. The analysis covers all 20 control families: AC, AT, AU, CA, CM, CP, IA, IR, MA, MP, PE, PL, PM, PS, PT, RA, SA, SC, SI, SR.

## 4.1 Access Control (AC)

### 4.1.1 `zencrypted/ias`: AC-2 — Account Management

The `ias` server (Identity and Access Server) is the platform's central Identity Provider (IdP), implementing the full account lifecycle through a single programmatic interface. Unlike fragmented LDAP directories, `ias` operates with declarative user profiles directly bound to the role registry in `roles.ex`.

**AC-2(1) — Automated System Account Management.** `ias` supports SCIM 2.0 (System for Cross-domain Identity Management) for automatic synchronization of account state across subsystems. When an event arrives from an HR module (e.g., ERP/EDU or ERP/HEALTH), `ias` automatically performs provisioning or de-provisioning without manual intervention, guaranteeing compliance with the Joiner-Mover-Leaver (JML) requirements.

**AC-2(2) — Removal of Temporary and Emergency Accounts.** Temporary accounts in `ias` have mandatory fields `expires_at` and `account_type: :temporary`. A background scheduler (implemented via Erlang/OTP `:timer`) inspects the database hourly and automatically deactivates expired records. Setting an expiration time is a required parameter when creating a temporary account.

**AC-2(3) — Disable Inactive Accounts.** The `ias` server stores a `last_seen_at` timestamp for each session. If the value exceeds a configurable threshold (default: 90 days), the account is transitioned to the `:inactive` state, with an automatic notification sent to the security administrator.

**AC-2(4) — Automated Audit Actions.** Any change in account state (creation, privilege modification, deactivation, deletion) generates a signed record

in the `kvs` audit log via event sourcing. This provides an immutable, cryptographically protected trail of all administrative actions.

**AC-2(5) — Inactivity Logout.** `ias` centrally manages session duration. The `session_idle_timeout` setting is a global parameter and can be overridden at the role level (e.g., a stricter 15-minute limit for administrators).

**AC-2(6) — Dynamic Privilege Management.** Since `ias` is integrated with `erpuno/abac`, privileges are not static profile attributes but dynamically computed decisions from the Policy Decision Point. This means elevated privileges (e.g., administrator mode for critical operations) are activated only for the duration of a specific session and for a specific resource.

**AC-2(7) — Role-Based Schemes.** The integration of `ias` with `roles.ex` allows roles to be organized hierarchically (RBAC). Role templates are inherited: the `auditor` role automatically receives all rights of the parent `read_only` role, without requiring duplication of rules.

**AC-2(8) — Dynamic Account Management.** For service accounts (machine-to-machine), `ias` supports OAuth 2.0 Client Credentials with short-lived tokens (TTL: 15 minutes). Services have no permanent password, eliminating the risk of long-term secret leakage.

**AC-2(9) — Restrictions on Use of Shared and Group Accounts.** The `ias` architecture does not allow creating "shared" accounts by default. Every subject — person or service — has a unique cryptographic identifier bound to an X.509 certificate issued by `synrc/ca`.

**AC-2(10) — Shared and Group Account Credential Change.** For technical group accounts (e.g., `ocsp_service`), `ias` implements a "secret rotation" mechanism triggered by every change in group membership, automatically generating a new key pair via `synrc/ca`.

**AC-2(11) — Usage Conditions.** Upon login, `ias` checks the currency of accepted terms of use. If the `terms_of_service_version` in the profile does not match the current version, access is blocked until the new terms are accepted.

**AC-2(12) — Account Monitoring for Atypical Usage.** Behavioral metrics (request frequency, geography, unusual hours) are aggregated by `ias` and forwarded to SIEM (Wazuh). When the behavioral baseline is exceeded, an incident is automatically created in `erpuno/itsm`.

**AC-2(13) — Disable Accounts of High-Risk Individuals.** SIEM integration allows `ias` to receive webhook signals about compromise. Upon receiving a `high_risk_account_detected` signal, the corresponding profile is transitioned to `:suspended` within one second, regardless of any currently active sessions.

#### 4.1.2 `zencrypted/ias`: AC-7 — Unsuccessful Logon Attempts

**AC-7 (Base Control).** `ias` maintains a counter of failed authentication attempts bound to the subject and IP address. After a configurable threshold (default: 5 attempts in 10 minutes), the account is temporarily locked (account lockout) with an automatic notification to the administrator.

**AC-7(2) — Purge or Wipe Mobile Device.** Upon receiving a signal from a Mobile Device Management (MDM) system about device theft or compromise, `ias` immediately revokes all tokens and certificates associated with that device via the OCSP revocation mechanism in `synrc/ca`.

#### 4.1.3 `synrc/ca`: AC-3 — Access Enforcement

The `synrc/ca` module implements the Reference Monitor (AC-25) — a centralized control mechanism that verifies every request to a protected resource based on X.509 certificates and ABAC policies.

**AC-3(3) — Mandatory Access Control.** `synrc/ca` supports data classification labels (Data Labels) in X.509 certificate extensions. This enables enforcement of the Mandatory Access Control (MAC) principle: a certificate with a `confidential` clearance level cannot access a resource labeled `secret`, even if an RBAC rule formally permits it.

**AC-3(4) — Discretionary Access Control.** Resource owners can delegate access rights via the attributed token mechanism of `ias`, implementing the classic DAC (Discretionary Access Control) model. Delegation is always bounded by the delegating subject's own permissions.

**AC-3(7) — Role-Based Access Control.** RBAC is implemented at the X.509 extension level, where the `SubjectAlternativeName` field contains role URNs. This means a role is cryptographically bound to a person and confirmed by the digital signature of the root CA, making forgery or substitution of a role technically impossible.

**AC-3(10) — Audited Override of Access Control Mechanisms.** For services using JWT or SAML, `ias` generates signed claims with a time-limited validity. `synrc/ca` acts as the authority issuing short-lived assertion tokens whose verification requires no query to the IdP (stateless verification).

**AC-3(11) — Restrict Access to Specific Information Types.** Isolation between ERP/1 tenants (e.g., between different courts or agencies) is implemented at the Kubernetes namespace level and through unique root certificates for each tenant, issued by `synrc/ca`.

**AC-3(12) — Assert and Enforce Application Access.** The `abac` access decision incorporates a set of attributes: `subject.role`, `subject.clearance`, `resource.classification`, `action.type`, `environment.time`, `environment.network_zone`. This ensures context-aware access in accordance with the Zero Trust principle.

**AC-3(13) — Attribute-Based Access Control.** Subject attributes are stored in `ias` and `synrc/ca`; resource attributes in KVS metadata. `abac` retrieves them at decision time, guaranteeing attribute freshness even under frequent context changes.

**AC-3(15) — Discretionary and Mandatory Access Control.** The system supports the simultaneous operation of two models: MAC (based on classification labels in X.509) and DAC (delegation via `ias`). MAC always takes priority: if a mandatory label denies access, a DAC rule cannot override it.

#### 4.1.4 `synrc/bpmn`: AC-4 — Information Flow Enforcement

The BPMN engine `synrc/bpmn` is the central orchestrator of business processes, and all information flows between platform components pass through it.

**AC-4 (Base Control).** Every data transition between business process tasks (BPMN Tasks) is a controlled event. `bpmn` implements "information gateways" — process nodes that verify data classification before transfer between network segments or tenants.

**AC-4(1) — Object Security and Privacy Attributes.** Artifacts (documents, case files) passed between tasks carry a mandatory `data_classification` attribute. The BPMN gateway rejects the transfer if the artifact's classification does not match the permitted level of the target process segment.

**AC-4(4) — Flow Control of Encrypted Information.** At boundaries between organizational units, `bpmn` performs schema validation of transferred documents (JSON Schema, XSD) and verification of CMS/XAdES signatures before continuing the process.

#### 4.1.5 `erpuno/abac`: AC-5 and AC-6 — Separation of Duties and Least Privilege

**AC-5 — Separation of Duties.** `abac` implements Separation of Duties (SoD) via declarative XACML-like rules specifying sets of mutually exclusive roles (SSD: Static Separation of Duties). For example, the same individual cannot hold both the `initiator` and `approver` roles for financial transactions. SoD rules are verified not only at action execution but also at role assignment — the system rejects an assignment that would create a conflict.

**AC-6 — Least Privilege.** The fundamental principle of `abac`: access is denied by default (Default Deny). Permission is granted only when an explicit, positive matching rule exists. Rules have the minimum necessary scope — bound to a specific resource, action, and context.

**AC-6(1) — Authorize Access to Security Functions.** Instead of static privilege grants, `abac` computes privileges dynamically based on current subject and context attributes. Elevated rights (e.g., BreakGlass mode operations) are temporary and automatically revoked after the critical operation completes.

**AC-6(2) — Non-Privileged Access for Non-Security Functions.** `abac` ensures that administrative roles (e.g., `security_admin`) do not have access to business functions (court records, medical data) by default. The security administrator administers *the system*, not *the data* of the system.

**AC-6(3) — Network Access to Privileged Commands.** Privileged commands (service restarts, configuration changes) are accessible only via a dedicated Management VLAN, not through the general network interface. `abac` checks the `environment.network_zone` attribute in every request.

**AC-6(4) — Separate Processing Domains.** For example, a CA registration operator may *submit* a certificate request, but only the CA administrator may *sign* it. This two-stage approval (Maker/Checker) is hard-coded in the BPMN process and ABAC rules.

**AC-6(5) — Privileged Accounts.** The list of privileged accounts (e.g., `global_root_admin`) is defined in `roles.ex` and subject to monthly audit (control AC-2(12)). The number of subjects in this group is minimized and documented.

**AC-6(7) — Review of User Privileges.** Quarterly, `ias` automatically generates a `privileged_access_review_report` listing all subjects with elevated rights, last-login dates, and anomalies. The report is forwarded to the CISO.

**AC-6(9) — Log Use of Privileged Functions.** Every execution of a privileged action is logged as a separate record in `kvs` with full context: subject, role, action, time, IP, hash of the executed command. These records are *immutable* due to the append-only nature of KVS.

**AC-6(10) — Prohibit Non-Privileged Users from Executing Privileged Functions.** Technically enforced through the combination of ABAC rules and X.509 cryptographic mandates: privileged API endpoints require the presence of a specific OID extension in the certificate, which is issued only upon explicit assignment of a privileged role.

## 4.2 Audit and Accountability (AU)

### 4.2.1 `zencrypted/ias`: AU-2, AU-3, AU-6, AU-9, AU-10, AU-12

**AU-2 — Event Logging.** `ias` is the primary source of most security events: login/logout, failed authentications, profile changes, privilege delegation. The event list is defined in configuration and complies with ND TZI 2.3-025-24 mandatory logging requirements.

**AU-3 — Content of Audit Records.** Each `ias` audit record contains: `timestamp` (millisecond precision, NTP-synchronized), `subject_id`, `event_type`, `resource_id`, `action`, `outcome` (success/failure), `source_ip`, `session_id`, `signature` (HMAC record signature).

**AU-6 — Audit Record Review, Analysis, and Reporting.** `ias` logs are automatically forwarded to SIEM (Wazuh) via secured syslog. Wazuh applies NIST and CIS correlation rules to detect anomalies and generate alerts.

**AU-9 — Protection of Audit Information.** Audit records are stored in `kvs` with DSTU 7564-2014 (Kupyna) hashing. Any unauthorized modification of a record is detected upon the next chain verification.

**AU-10 — Non-Repudiation.** Critical events (document signing, approvals, certificate issuance) are recorded with RFC 3161 TSP timestamps from a trusted TSA provider, guaranteeing the legal evidentiary weight of records in judicial proceedings.

**AU-12 — Audit Record Generation.** `ias` generates audit records in real time for all configured events. A logging failure (e.g., due to buffer overflow) causes the operation itself to fail — the "Fail Secure" principle.

## 4.3 Assessment, Authorization, and Monitoring (CA)

### 4.3.1 `synrc/ca`: CA-2, CA-6, CA-7, CA-8, CA-9

**CA-2 — Control Assessments.** `synrc/ca` automates the collection of compliance evidence via the CMDB API. Before each audit (DSSZZI state expertise), `mix run -e 'CA.TeX.generate()'` is executed, generating a complete documentation package from the current system state.

**CA-6 — Authorization.** System authorization is formalized through the L3 security profile (`legal_l3_profile_erp.pdf`), programmatically generated from the CMDB and cryptographically signed. Authorization is updated upon any significant architectural change.

**CA-7 — Continuous Monitoring.** Continuous monitoring is implemented through a triad: Wazuh SIEM (security events), Zabbix (availability and performance), and `synrc/ca` CMDB (configuration compliance). Any deviation from the recorded baseline state (CMDB drift) immediately generates an incident in `itsm`.

**CA-8 — Penetration Testing.** Regular penetration tests (at least annually) cover all ERP/1 components. Results are formalized as CMDB risk records and tracked through Plan of Action & Milestones (POA&M — control PM-4).

**CA-9 — Internal System Connections.** All internal connections between ERP/1 services are authorized via mTLS (mutual TLS) with certificates from `synrc/ca`. An unauthorized or non-certificated connection is technically impossible.

## 4.4 Configuration Management (CM)

### 4.4.1 `synrc/ca` CMDB: CM-2, CM-3, CM-6, CM-7, CM-8, CM-9

**CM-2, CM-3 — Baseline Configuration and Configuration Change Control.** The baseline configuration of all components is captured in CMDB Elixir modules (`hw.ex`, `sys.ex`, `net.ex`). Every change in the production environment must first be reflected in the corresponding CMDB file and pass Code Review in Git. Deviation from the baseline (configuration drift) is detected by Wazuh FIM (File Integrity Monitoring).

**CM-6 — Configuration Settings.** All ERP/1 services are launched with strict security hardening baselines: UA Linux DSTU-hardened, SELinux Enforcing, Windows Server DISA STIG. Deviations from baseline settings are technically blocked through SCM mechanisms (Puppet/Ansible).

**CM-7 — Least Functionality.** Each ERP/1 service runs only with the components required to perform its function. Unnecessary modules, protocols, and ports are disabled. The list of permitted components is documented in the corresponding `sys.ex` CMDB entry.

**CM-8 — System Component Inventory.** The `synrc/ca` CMDB is a "living" registry of all hardware, software, and network components. Each resource has a unique inventory number, bound to a cryptographic certificate and recorded in `hw.ex` or `sys.ex`.

**CM-9 — Configuration Management Plan.** Instead of a separate textual document, the CM plan is directly encoded in the Git repository: the CI/CD pipeline, Elixir CMDB modules, Ansible playbooks, and this PDF report together form a complete, self-verifying configuration management plan.

## 4.5 Contingency Planning (CP)

### 4.5.1 `erlang/otp`: CP-2, CP-7, CP-9, CP-10

**CP-2 — Contingency Plan.** Erlang/OTP is the foundation of ERP/1 fault tolerance. The Supervision Tree architecture guarantees the automatic restart of any failed process. At the cluster level, a minimum of three nodes (quorum) ensures availability even upon failure of one node.

**CP-7 — Alternate Processing Site.** Erlang/OTP supports hot failover between cluster nodes without loss of current sessions. The distributed process registry (`:pg` or via `synrc/kvs`) allows another node to take over processing upon primary node failure.

**CP-9 — Information System Backup.** `kvs` data is continuously replicated to all cluster nodes (synchronous Mnesia/RocksDB replication). Daily snapshots are written to a tape archive (HPE StoreEver) for offline storage.

**CP-10 — Information System Recovery and Reconstitution.** Recovery procedures are rehearsed as part of training (AT-3) in an isolated environment. The built-in `:hot_code_upgrade` function allows components to be updated without system downtime, minimizing RTO (Recovery Time Objective).

## 4.6 Identification and Authentication (IA)

### 4.6.1 `synrc/ca` + `zencrypted/ias`: IA-2, IA-5, IA-8

**IA-2 — Identification and Authentication (Organizational Users).** `ias` enforces strict MFA: the first factor is an X.509 certificate (smart card or IIT Gryada HSM token), the second factor is an OTP (TOTP/HOTP or hardware token). No system function is accessible without successful completion of both factors.

**IA-2(1) — MFA for Privileged Accounts (Network Access).** Administrative accounts additionally require a third factor — push-notification confirmation on a registered device. Login from a "shared" device is technically blocked.

**IA-2(2) — MFA for Non-Privileged Accounts.** Standard users authenticate with a minimum of two factors. The first is a certificate on a smart card (PKCS#15, DSTU 4145-2002 algorithm), the second is the smart-card PIN.

**IA-5 — Authenticator Management.** `synrc/ca` is the authoritative source of cryptographic authenticators (certificates). Management includes: enrollment (Certificate Enrollment via EST), renewal (ACME/CMP), revocation

(OCSP/CRL), and archiving (Long-Term Validation, LTV). All authenticators are bound to a hardware carrier (e-Token, Gryada-301).

**IA-5(1) — Password-Based Authentication.** For service accounts where passwords are still used, `ias` enforces minimum complexity and stores passwords in Argon2id format (PHC winner, resistant to GPU attacks). Passwords are never transmitted in plaintext.

**IA-8 — Identification and Authentication (Non-Organizational Users).** For external systems (e.g., Unified State Register, Diia), `ias` supports identity federation via SAML 2.0 and OIDC, where the external IdP verifies the identity and `ias` issues a local token with limited rights based on attributes received from the external provider.

## 4.7 Media Protection (MP)

### 4.7.1 `synrc/kvs`: MP-2, MP-4, MP-5, MP-6, MP-7

**MP-2, MP-4 — Media Access and Storage.** `kvs` is the primary storage for all critical ERP/1 data. Data is encrypted at the record level using DSTU algorithms (Kalyna AES-256 GCM) with keys stored in an IIT Gryada HSM. Physical access to servers running `kvs` is restricted via the Policy Engine and PE controls.

**MP-5 — Media Transport.** Tape backups (HPE MSL3040) are encrypted before writing. Physical tapes are stored in a safe with dual control. The procedure for removing a tape from the perimeter requires an authorized CR in `itsm`.

**MP-6 — Media Sanitization.** The sanitization procedure (DoD 5220.22-M or physical destruction for SSD/flash) is documented in `itsm` and recorded in the CMDB as a component de-inventory event.

**MP-7 — Media Use.** Removable media (USB) usage is technically blocked at the OS level (udev rules, Group Policy) for all workstations, except specifically authorized technical workstations with CISO approval.

## 4.8 System and Communications Protection (SC)

### 4.8.1 `synrc/vpn`: SC-7, SC-8, SC-12, SC-28

**SC-7 — Boundary Protection.** `synrc/vpn` implements a strict network perimeter based on IPsec IKEv2 with X.509 certificate authentication. All external connections (between sites, with remote users) pass through VPN tunnels. The Cisco Firepower 4145 NGFW (documented in CMDB) filters traffic at the perimeter.

**SC-7(3) — Access Points.** The number of external network connections is minimized and strictly documented in the `net.ex` CMDB. Each new access point requires a separate CR and CISO approval.

**SC-8 — Transmission Confidentiality and Integrity.** All traffic between ERP/1 components is protected by mTLS 1.3 with mandatory DSTU-

compatible cipher suites. Unencrypted traffic is technically impossible — `ias` rejects requests without a valid TLS certificate.

**SC-12 — Cryptographic Key Establishment and Management.** `synrc/ca` is the authoritative key center. Root keys are stored exclusively in the HSM (Gryada-301) and never leave the hardware module. Key rotation is performed according to the Key Ceremony procedure with Dual Control.

**SC-28 — Protection of Information at Rest.** PostgreSQL and Oracle use TDE (Transparent Data Encryption) with keys from the HSM. `kvs` performs additional encryption at the record level.

## 4.9 System and Information Integrity (SI)

### 4.9.1 `synrc/chat`: SI-3, SI-4, SI-7, SI-10

**SI-3 — Malicious Code Protection.** All cluster nodes are protected by Wazuh HIDS with up-to-date signatures. At the CI/CD pipeline level, automatic dependency scanning (SBOM, OWASP Dependency Check) is executed on every commit.

**SI-4 — System Monitoring.** The combination of Wazuh (security events) and Zabbix (performance metrics) provides 24/7 monitoring of all components. The Wazuh event correlator detects attack patterns (MITRE ATT&CK) and automatically escalates them to `itsm`.

**SI-7 — Software, Firmware, and Information Integrity.** All ERP/1 releases are signed with a DSTU 4145-2002 digital signature from `synrc/ca` and published together with signatures. Checksums (DSTU 7564-2014 Kupyna-512) are verified before installing any update.

**SI-10 — Information Input Validation.** `synrc/chat` and all ERP/1 web components (via `synrc/ws`) apply strict schema validation (JSON Schema / XSD) of input data at the API Gateway level before passing it to business logic.

## 4.10 Supply Chain Risk Management (SR)

### 4.10.1 `synrc/chat` + `synrc/ca`: SR-3, SR-4, SR-11

**SR-3 — Supply Chain Controls and Processes.** ERP/1 uses exclusively open-source components (Erlang/OTP, Elixir), whose source code is verified before inclusion. An SBOM (Software Bill of Materials) is generated automatically at every build.

**SR-4 — Provenance.** All components have cryptographically verified provenance. Release signatures are verified through the `synrc/ca` root CA. An undocumented or unsigned component cannot be installed in the production environment.

**SR-11 — Component Authenticity.** Hardware components (HSM, switches, servers) are verified via serial number and CMDB inventory record. Vendors (5HT Technology, IIT, Cisco) have signed supply chain security agreements.

# 5 Conclusion

By treating the Information Security Management System (ISMS) and the KSZI documentation as "Infrastructure as Code" (IaC) via Elixir maps, ERPUNO LLC achieves a continuous, verifiable, and strictly compliant security posture. This approach significantly reduces the friction typically associated with DSSZZI and NIST audits by ensuring that the actual state of the system is always perfectly synchronized with its certified documentation.

### 5.1 Codebase Overview for Copyright Registration

The entire Configuration Management Database (CMDB), Continuous Accountability System, and PKI Certificate Authority components discussed in this document are implemented as a cohesive software suite. This software suite forms the basis for the formal registration of the copyright work.

The core architectural blocks of the codebase include:

- **SYS-SYNRC-CA**: The central Certificate Authority and HSM backend responsible for issuing X.509 certificates, OCSP, CRLs, and managing the entire PKI lifecycle via ACME and EST protocols.
- **CMDB Profiles**: The declarative Elixir modules defining the precise state of hardware (`hw.ex`), network topology (`net.ex`), and system applications (`sys.ex`).
- **Policy and Risk Engines**: Modules responsible for automated data categorization (`data.ex`), dynamic risk taxonomies (`risk.ex`), and strict role-based/attribute-based access controls (`roles.ex`, `abac.ex`).

The software is continuously developed, documented, and published at the following official resources:

- **Source Code Repository**: `https://github.com/synrc/ca`
- **Official Product Portal**: `https://erp.uno/ca/`
- **Developer Documentation**: `https://ca.n2o.dev`

## References


[1] National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53, Revision 5.

[2] Державна служба спеціального зв'язку та захисту інформації України. *НД ТЗІ 3.7-003-2023. Порядок проведення державної експертизи в сфері технічного захисту інформації.*

[3] Державна служба спеціального зв'язку та захисту інформації України. *НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.*

[4] International Organization for Standardization. *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.*