INTESA SANPAOLO

Audit PKI SSL Report
Innovery S.p.A.

Summary

1. FOREWORD

In the period between June 6 2016 to 15 July 2016, Intesa SanPaolo Certification Authority has been under an audit procedure for their PKI issuing SSL digital certificates, to assess its conformity to the current CAB Forum requirements. The audit related information and outcomes are herewith specified.

The audited personnel are located at the Intesa SanPaolo S.p.A. (here in after, Intesa SanPaolo) in Milan. PKI main sites are in Moncalieri (Turin) and Settimo Milanese (Milan); the disaster recovery site is located in Parma, suitably far from the main sites.

The PKI implements a “one tier” model, based on a single level of Enterprise CA which includes Policies and Issuing CA rules. Actually, PKI includes two CAs (CA Servizi Esterni and CA Servizi Esterni Enhanced) which are subordinated to a root external CA hosted by DigiCert. While CA Servizi esterni does not release certificates anymore, and it is maintained up and running only for the purpose of issuing CRL, CA Servizi Esterni Enhanced is used to release new DVCP and OVCP certificates.

All sites are under strict security surveillance by a private security agency, making therefore extremely difficult for an external person to enter into the premises. Besides, it is worth mentioning that the Intesa Business Continuity Plan is used in the ISO/IEC 27000 enviroment as one of the two paradigm BCPs to wich BCPs should be inspired. Therefore, being the PKI Disaster Recovery included within such BCP, it was deemed superfluos to visually assess its enforced measures.

This Audit procedure is performed under the CA/Browser Forum Baseline Requirements specification, clause 8.4 point 2 (ETSI EN 319 411-1 scheme).

1.1 ROLES REFERENCES

Role	name
Editor	Innovery SpA - http://www.innovery.net
Author	Guido Moscarella
Approval	Gianvittorio Abate
Authorized	Gianvittorio Abate

1.2 VERSIONS

Version id	descrizione
0.0.1	First draft
1.0.0	Final Release

1.3 DEFINITIONS

For the purposes of the present document, the terms and definitions given in ISO/IEC 17065 [1] and the following apply:

auditor: person who assesses conformity to requirements as specified in a given requirements document

competence: ability to apply knowledge and skills to achieve intended results

conformity assessment: process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled

NOTE: From Regulation (EC) No 765/2008 [i.4] and section 2.1 of ISO/IEC 17000:2004 [i.5].

conformity assessment body: body that performs conformity assessment services which is accredited as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides

NOTE: This is equivalent to conformity assessment body as specified in point 13 Article 2 of Regulation (EC) No 765/2008 [i.4].

national accreditation body: sole body in a State that performs accreditation with authority derived from the State

NOTE: This is equivalent to national accreditation body as specified in point 11 Article 2 of Regulation (EC) No 765/2008 [i.4].

technical expert: person who provides specific knowledge or expertise to the audit team

NOTE 1: Specific knowledge or expertise relates to the organization, the process or activity to be audited, or language or culture.

NOTE 2: A technical expert does not act as an auditor in the audit team.

trust service: electronic service which enhances trust and confidence in electronic transactions

NOTE: Such trust services are typically but not necessarily using cryptographic techniques or involving confidential material.

Trust Service Provider (TSP): entity which provides one or more electronic trust services

1.4 ABBREVIATIONS

For the purposes of the present document, the following abbreviations apply:

CA Certification Authority

CAB	Conformity Assessment Body
EC	European Commission
EU	European Union
ISMS	Information Security Management System
IT	Information Technology
TSP	Trust Service Provider
NCP	Normalized Certificate Policy
NCP+	Normalized Certificate Policy requiring a secure cryptographic device
LCP	Lightweight Certificate Policy
EVCP	Extended Validation Certificate Policy
DVCP	Domain Validation Certificate Policy
OVCP	Organizational Validation Certificate Policy

1.5 REFERENCES

id	name	description
1	en_319403v020202p.pdf	ETSI document EN 319 403 V2.2.2
2	en_31941101v010101p.pdf	ETSI document EN 319 411-1 V1.1.1
3	en_31940101v020101p.pdf	ETSI document EN 319 401-1 V2.1.1
4	CA-Browser-Forum-BR-1.3.7.pdf	Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates
5	EN319411-1v111-checklist.xlsx	Check list pertinent to ETSI EN 319 411-1 V1.1.1

2. STRUCTURE OF THIS REPORT

According with standard ETSI EN 319 411-1, referenced in [2], this audit will report the following information:

a) an account of the audit including a summary of the document review and the standard(s), publicly available specifications and/or regulatory requirements against which the audit is carried out (see clause §3, §4, §6);

b) an account of the audit of the TSP's information security risk analysis (clause §4.1);

c) total audit time used and detailed specification of time spent on document review, assessment of risk analysis, on-site audit, and audit reporting (see clause §3.1);

d) audit enquiries which have been followed, rationale for their selection, and the methodology employed including sampling methodology and test procedures (see clause §4).

Others report details, related to areas covered by the audit, observations, details of any nonconformities identified and comments on the conformity of the TSP and the trust service, are reported in clause §6.

Finally, conclusions about the outcome of this Audit, is reported in clause §6.

3. AUDITING PROCEDURE

3.1 AUDIT TIME

The Audit work that brought to this report took about 2 months.

On 6 of June the audit began with an opening meeting between the auditing team and the audited one, which goal was to outline the audit activities.

On 10 of June, the Auditee shared all the stage 1 documents related to the TSP activity.

From that point until 27 of June, the Audit team reviewed those documents releasing Stage 1 report (see §4).

From 4 of July, the audit process starts with Stage 2. On 5 of July there has been a meeting in Moncalieri where local interviews were performed.

On 26 of July, the audit final meeting was held and this report was reviewed with the Client.

3.2 AUDIT PROCESS

The objective of the audit process is to confirm and certify that Intesa SanPaolo and the trust services it provides, comply with the applicable assessment criteria.

The audit process followed an initial preparation step, in which the TSP Intesa SanPaolo did all the necessary arrangements for the conduct of the audit including the provision of the relevant documentation.

This Audit has been performed in two stages:

- **Stage 1:** This stage focused on obtaining and reviewing the documentation on the TSP and the TSP's audited service(s).
- **Stage 2:** This stage focused in an on-site audit to validate the preliminary audit report findings.

3.2.1 STAGE 1

This stage is focused on obtaining and reviewing the Intesa SanPaolo and its trusted service(s) documentation.

The objective of audit stage 1 was to provide a focus for planning of audit stage 2 by gaining an understanding of the structure and extent of the Intesa SanPaolo audited service(s).

For this reason, the Auditor team has analysed the following Intesa San Paolo documents:

1. Technical PKI architecture documents:
    a. Architettura_Intesa Sanpaolo - Certification Authority - v2.0_20160607
2. Business continuity documents:
    a. IGS-IGG6721048 DC SIST HELP DESK TECNOLOGICO-MNCSav_it-it
    b. IGS-IGG6721048 DC SIST HELP DESK TECNOLOGICO-NAMarc_it-it
    c. IGS-IGG6721071 DC SIST GESTIONE SICUREZZA INFORMATICA-MIBisc_it-it
    d. IGS-IGG6721071 DC SIST GESTIONE SICUREZZA INFORMATICA-MNCSav_it-it
    e. IGS-IGG6721071 DC SIST GESTIONE SICUREZZA INFORMATICA-NAMarc_it-it
    f. IGS-IGG6721048 DC SIST HELP DESK TECNOLOGICO-MNCSav_it-it
3. CPS:
    a. ISP-GSC-311-2015-02 Certification Practice Statement Enhanced
4. Intesa San Paolo organizational structure:
    a. Matrice ruoli CA_v2_20160607
    b. Organigramma Area strategie operative (00000004)
5. Access control:
    a. Regole di sicurezza fisica – 2016
    b. Regole di sicurezza fisica per stabili centrali e sedi direzionali - 2016
6. Information Security management
    a. Regole di sicurezza per la Protezione del Patrimonio Informativo
7. Networking:
    a. Regole di sicurezza per le reti - 2016

All the collected documents are up to date, and reviewed on a regular basis.

3.2.1.1 STAGE 1 FINDINGS

From the analyzed documents reviewed at stage 1, no “no conformities” was found, nor observations and recommendations to reports.

3.2.2 STAGE 2

Stage 2 assessment demonstrates compliance of its operations for all relevant TSP processes with the claimed standard and common state of the art security measures.

From security perspective, it was verified that staff protocols and risks management measures were in place.

Audit team visited PKI rooms in Moncalieri, and verified technical, logical and physical measures were in place; this includes:

- Man trap measures;
- Pass back system;
- Badge control check;
- CCTV;
- Power and air conditioning;
- Water exposure;
- Fire prevention and protections;
- Media storage security measures;
- Waste disposal;
- Oversight by security personnel on site.

Physical policies are in place in order to avoid grant access to unauthorized personnel. Accesses are verified with proximity badge/readers technology.

Logical access to CA are also in place, implemented to RBAC (Microsoft Domain) rigorous policies.

From CA perspective, it was also verified that HSM are under strict and secure control measures; this includes and HSMs appliances are under dual plug power supply, installed in rack with security measure.

No “no conformities” were founded; no further measures must be taken.

4. OTHER INFORMATIONS SOURCES

4.1 ACCOUNT OF INFORMATION SECURITY RISK ANALISYS

Intesa SanPaolo has internal processes compliant to ISO 27001. Policies and procedures are then assured by Internal Intesa SanPaolo departments at all levels.

All security controls are implemented in order to address this security policy and its enforcement.

RBAC access policies are fully applied to logical and physical levels, in order to assure that grants assigned to a user, are tailored to his needs. Security roles nomination (administrator), are communicated through proper letters of appointment.

Security Risks are prevented through a mature approach that includes the adoption of very high security standard to design environment of IT systems.

The risk assessment process is annually reviewed and revised, at renew of ISO 27001 certification. At the same time residual risks are treated in order to comply with reduction's risks requirement.

4.2 AUDIT ENQUIRIES

Other information was collected through audit enquiries, that were conducted during Stage 2 with the auditee's persons in charge of the following responsibilities:

- Certification Authority
- Business continuity plan
- Incident management
- Change management
- Security Assessment
- Access control
- Information security manager

A physical survey was performed on the outer PKI room security measures, in order to verify compliance with the standards.

4.3 SAMPLE OPERATIONS

Supervision on sample operation on the PKI performed by the auditee's personnel under request by the auditing team. It was positively verified that:

- the machine room access log is properly maintained: this was verified on a sampling basis;
- the CA Log is properly maintained: this was verified on a sampling basis;
- the certificate profile specifies an Extended Key Usage extension for Server Authentication;
- it was found that the certificates specify URI through which the CPS can be fetched.

5. NON CONFORMITIES, OBSERVATIONS, RECOMMENDATIONS

1. Non Conformities
    - No "Non Conformities" was found;
2. Observations
    - There are limited observations to report:
        a. CPS must comply with this new Audit scheme (ETSI EN 319 411-1);
        b. CPS must state a clause conform to ETSI EN 319 411-1 clause 5.2d, that disclose its CPS through an online means that is available on a 24x7 basis;
        c. OCSP conformances metioned in CPS must be updated with new one (RFC 6960).
3. Recommendations
    - No relevant recommendations to report.

6. FINDINGS AND CONCLUSIONS

The auditing team deems "Intesa SanPaolo - Servizio di certificazione Digitale" is meeting all necessary requirements pertinent to ETSI EN 319 411-1, in force at the date of audit.

The auditee has been found as satisfactorily compliant with the reference normative.

The overall auditee security measures are assessed as very good.

Detailed report checklist related to the audit activity, it is provided in document ref [5].