Security target C.S.P.N.

Electronic SAFE D3S

About IDEMIA

OT-Morpho is now IDEMIA, the global leader in trusted identities for an increasingly digital world, with the ambition to empower citizens and consumers alike to interact, pay, connect, travel and vote in ways that are now possible in a connected environment.

Securing our identity has become mission critical in the world we live in today. By standing for Augmented Identity, we reinvent the way we think, produce, use and protect this asset, whether for individuals or for objects. We ensure privacy and trust as well as guarantee secure, authenticated and verifiable transactions for international clients from Financial, Telecom, Identity, Security and IoT sectors.

With close to €3bn in revenues, IDEMIA is the result of the merger between OT (Oberthur Technologies) and Safran Identity & Security (Morpho). This new company counts 14,000 employees of more than 80 nationalities and serves clients in 180 countries.

Document Management

Target audience

Audience	Subject
General public	Information on D3S product CSPN

Document revision

Date	Revision	Modification	Created by
2021/06/23	1.0	Public target document	Idemia

Table of Content

1. Introduction

1.1. Object of this document

This document is the security target for the first level security certification (C.S.P.N.) of the ***Digital Secure Storage Server (D3S)*** (digital safe) for this certification by the National Agency for Information Systems Security. The security functions described here, close to the requirements of the Regulator Authority for Online Games (ARJEL), are however likely to respond to many other use cases and are not limited to the only requirements relating online games.

1.2. Definitions

Locker

A Locker is a set of safe boxes dedicated to a group of identified users.

Autority

Abstract term for the body responsible for auditing traces.

Coffre (safe box)

A Safe box/safe is the basic storage space of D3S: it is within a Locker that gaming records are stored and that traceability of operations relating to it is ensured.

Deposit

The act of adding one or more gaming records to D3S. Any deposit results in the generation of a deposit proof to ensure the auditability of the operations carried out and their restitution to the authorized roles.

Trace / Secret

Trace is a batch of one or more gaming records (sent by the captor) for which a deposit proof is created and which are stored in SAFE. We talk about a trace or secret to indicate a gaming record in encrypted form.

Export

Exporting consists of extracting traces from the D3S (without data decryption, unlike restitution (see below)).

Operator

Organization audited by the authority.

Gaming records

A gaming record consists of the data deposited in the safe during a deposit operation. The operation on the SAFE is independent of the nature and format of this data, and its role is to ensure its integrity and confidentiality.

A gaming record is uniquely identified in D3S.

Also called “gaming event” or “archived information package” (according to the specifications on the A.N.S.S.I. (ref. SGDN/DCSSI/SDO/BCS)).

Deposit proof

In order to ensure the traceability of the operations carried out (e.g: deposits and withdrawals), the SAFE keeps, for each deposit, a certain number of information making it possible, for example, to charge the deposit to a given user, check the order of these operations, etc.

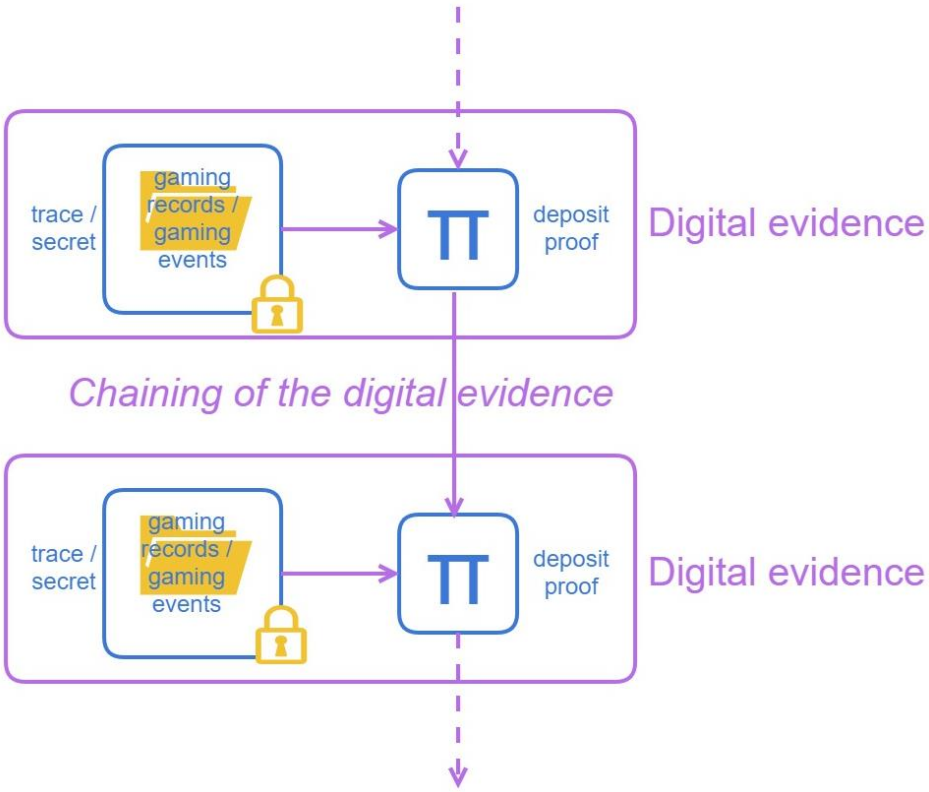
This information is called “evidence” when there is no fear of confusion.

Restitution

Reading act (data access) of one or more previously field digital documents. Restitution involves decryption of the trace containing the gaming record (reading and access to data).

Digital evidence

A digital evidence consists of a trace and its associated deposit proof.



2. Identification of the product

Publishing organization	IDEMIA
link to the organization	www.IDEMIA.com
Product trade name	*Digital Secure Storage Server (D3S)*
Evaluated version number	5.5.0.65
Product category	9 – secure storage

3. Arguments

The context of use corresponds to the monitoring of the transactional activities of an entity named "operator" by an "authority". The authority wishes to control certain operations within the operator's information system and validates for this purpose a technical device which is the service responsible for collecting and archiving digital evidences of these operations.

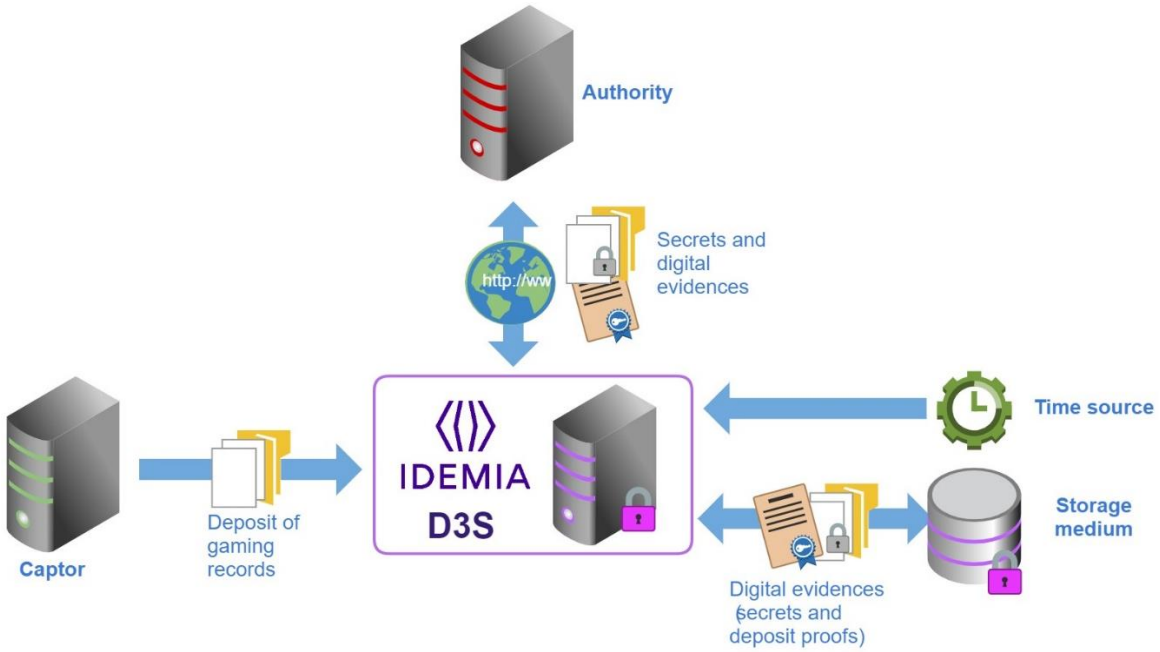
D3S is a component of a technical device responsible for guaranteeing the traceability of operations carried out on the information system. This device consists of a captor and the **D3S**. The captor, outside the scope of this document, is responsible for collecting the traced data. This data is than archived in the digital SAFE to guarantee its integrity and completeness over time. Before the data is transmitted to the authority, the **D3S** records the data and seals it so that it cannot be altered, making any addition, deletion or modification of transaction detectable.

D3S ARJEL Client (d3sc) is the client tool of the Digital Secure Storage Server SAFE API, which allows data to be exported from the SAFE, guaranteeing its confidentiality and integrity.

The storage medium is not part of D3S in the sense that the security properties (confidentiality, integrity, chaining) of the data controlled by the SAFE are independent of the storage system (file system, database, etc…).

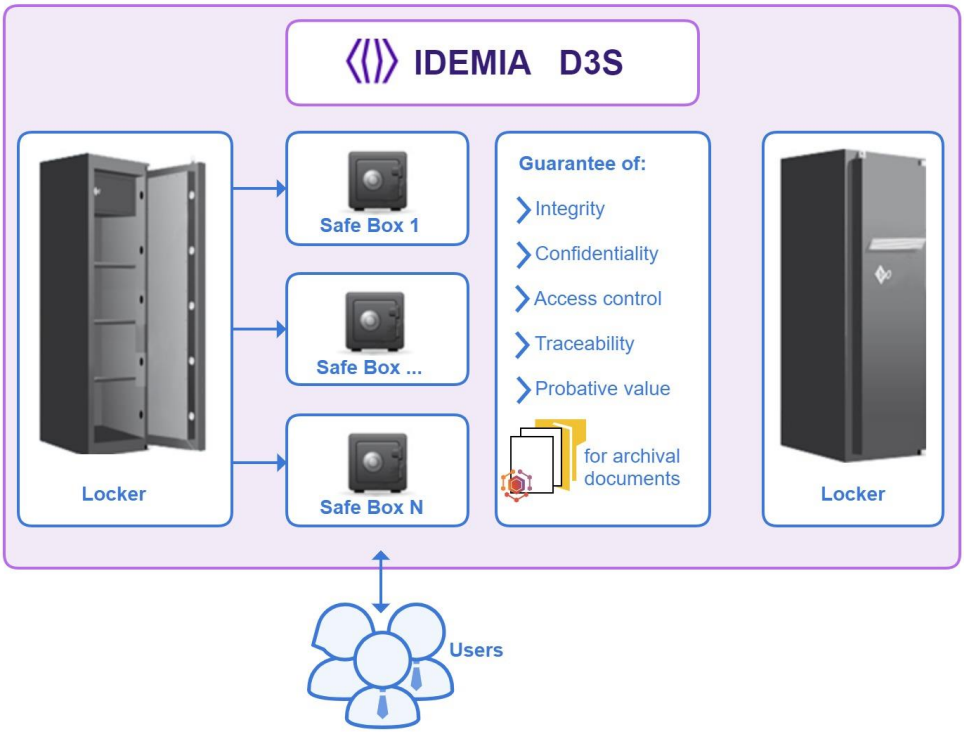
3.1. Functionnal Description

3.1.1. General architecture



3.1.2. D3S

D3S, the server part of the product, is organized on the same principle as a physical **safe room**: there are Lockers, these Lockers themselves containing one or more **safe boxes**.
Each of the safe boxes can either be empty or contain one or more **traces.**



D3S is assumed to be installed and configured as part of a controlled process (see below for details on how to bring the **D3S** into production).
D3S relies on a secure storage medium and, reasonably, on a physical containment of the cryptographic secrets it uses (sealing). These cryptographic secrets are identified as elements of the environment in the assumptions of section 3.2.1.2.

3.1.2.1. Configuration of D3S (administration)

The management of profiles, keys and various parameters of the **D3S** is carried out by administrators.

An administrator has no rights over the contents of the SAFE.

3.1.2.2. Users and profiles

Once installed, **D3S** interacts with different users, who are associated with different profiles:

- The Depositor: this is the application client (software) responsible for recovering the data to be traces. This user authenticates with the **D3S** with the ***"depositor"*** profile.
- Officers with control and audit powers. They authenticate with the **D3S** with a ***"reader"*** profile. It can be individuals or software.
- The agents (individuals) responsible for managing the profiles. They authenticate with the **D3S** platform as an **"administrator"** profile.

Profile	User	Operations and rights
Depositor	Captor	• Deposit of gaming records • Verification of the integrity and completeness of the deposit proofs
Reader	Audit and control officer	• Recovery of encrypted gaming records (export) • Verification of the integrity and completeness of the deposit proofs and traces.
Administrator	Authority or designated by Authority	• Initial configuration of the safe • Updates of the profile

The **D3S** makes it possible to configure several distinct **"safe boxes"** (storage spaces), each safe box having a set of users and potentially partitioned profiles: rights, profiles and users are understood by safe box.

These authorized actions for each profile are distinct (thanks to partitioning of roles). Thus, for example, a reader cannot deposit documents and conversely, a depositor is unable to read any digital document.

In addition to those profile, the technical operators (natural persons) responsible for the daily operation of the **D3S** under the responsibility of the **D3S** platform operator, also interact with the **D3S** and its environment (network, hardware, platform setup and restart, retrieval of log and anonymous operation reports, etc.).

These staff have no functional role vis-a-vis the **D3S**.

User	Operations and rights
Technical Operators & monitoring system	• Daily operation : stop, restart • Access to monitoring (operational status of the service) and log interface

3.1.2.3. Deposit (use)

In current operation, the *"depositors"* authenticate themselves after **D3S** and deposit gaming records there. The deposit of a gaming record in the **D3S** take place as follows:

1. Encryption of the gaming record (creation of the trace)
2. Generation and sealing of the associated deposit proof (creation of the digital evidence)

A depositor can't read the deposited documents (including its own) and can't access the configuration of the **D3S** as well. He can **ONLY** access the deposit proof of the documents he has filled.

3.1.2.4. Audit (use)

In current operation, the *"reader"* users authenticate themselves against **D3S** then access the traces (export of encrypted data) of gaming records deposited and the associated proofs. A reader can't modify the deposited documents and can't access the configuration of the **D3S**.

3.1.2.5. Administrator (certificate and profile update)

When one of the certificates needs to be updated, the *"Administrator"* users can connect to the GUI of **D3S** to replace one of the certificates with a newer version or modify the profile list.

Warning : Any modification of the profile list requires to update the configuration file to keep it synchronized with the result after modification.

3.1.3. D3S ARJEL Client (d3sc)

D3S ARJEL Client (d3sc) is the client tool in the D3S safe, which exports to a secure transport archive and then allows local data to be extracted in clear from this archive validating their integrity.

d3sc has no privileged access to the APIs of the D3S safe, it is a utility which facilitates the use of the D3S safe and offers the guarantee that its certified implementation as part of the D3S product is properly using all security functions to ensure the integrity of data.

D3S ARJEL Client (d3sc) must be installed and configured as a part of a controlled process (see below for the details of putting the **D3S ARJEL Client** into production.

3.1.3.1. Installation and initialization

The **D3S ARJEL Client (d3sc)** is delivered by IDEMIA to the authority.

- The archive decryption key is generated and stored in a software store. The user, for this part, has access only to the public key which corresponds to this decryption key.
- The authority only has a reader profile.

Physical protection

Physical access to the machine on which **D3S ARJEL Client (d3sc)** is hosted is under control of the Authority, which makes sure to prevent any access by a malicious user.

3.1.3.2. Users and profiles

Once installed, **D3S ARJEL Client (d3sc)** interacts with D3S via a *"reader"* profile. The configuration of the installation of the **D3S ARJEL Client (d3sc)** only allows the use of a single fixed user profile, of the *"reader"* type. Its export functionality is only possible for this profile.

3.1.3.3. Export (use)

The export command of the **D3S ARJEL Client (d3sc)** uses the certificate configured during installation to authenticate after D3S and exports the secure transport archives which contain the encrypted data and associated proofs.

3.1.3.4. Star (use)

The *star* command of the **D3S ARJEL Client** allows the manipulation of secure transport archives which have been exported from D3S. It deciphers the data, validates each deposit proof, and checks the integrity of their chaining.

Note : The **D3S ARJEL Client** provided can also be used as a simple to use tool to deposit gaming deposit to the **D3S** product, but in the real operation environment, this is done directly by the captor of the gaming operator, and this functionality isn't part of the evaluated scope.

3.2. Technical environment

3.2.1.1. Hardware and Software

D3S relies on the following:

- A storage medium (disks, database, etc.) where the traces and deposit proofs are recorded.
- A hardware confinement (hardware security module) of cryptographic secrets (in particular, the signature key used for the sealing of parts and traces)
- A reliable source of time.

D3S ARJEL Client (d3sc) relies on the following:

- a storage medium (disks) on which the secure transport archives are saved,
- a storage of cryptographic secrets (in particular, the decryption key)

3.2.1.2. Description of the environmental assumptions

EA1. Captor

The captor is a software and a hardware infrastructure responsible for capturing and depositing traces corresponding to the activity of the depositor (operator). This captor is assumed to be independently certified to demonstrate proper operation. Therefore, this captor is assumed to be trusted, which includes following assumptions:

- The captor only submits authentic documents (corresponding to real transactions and not, for example, random data or dummy operations)
- The D3S-captor platform is correctly sized to support the operator's operational constrains (no risk of denial of service due to saturation of storage spaces, bandwidth or processing capacity).

The captor interprets the responses (or the absence of a response) from the D3S as to resubmit, if necessary, a deposit for which it has not received an acknowledgment.

EA2. Decryption private key

The deposit decryption private key cannot in any case be communicated to the operator (i.e. its captors) who only knows the public part of this key for encrypting. This private key is fully controlled by the issuing authority (ANJ) and securely stored in its HSM or smart card. Only ANJ agents with control and audit powers can use this key.
The decryption of traces using this key is handled by the D3S ANJ Client tool.

EA3. Installation and initialization

The **D3S** is installed by IDEMIA and then configured for a given operator under the supervision of the authority in a configuration ceremony.

- The proof of sealing key is generated and stored in HSM (hardware security module)
- The encryption key is configured in an application manner (public key).
- The users and their profiles are configured. The operator only has a deposit profile.
- The OS is hardened by the use of separate administrator user accounts (root) and D3S operator (d3s). The D3S technical operator only has access to the operating functions (stop, start, download of technical logs). The use of strong passwords (in accordance with the CERTA information note "CERTA-2005-INF-001") is particularly recommended. The keys for log export and monitoring access are configured and communicated to technical operators.
- *"root"* identifiers and passwords are not communicated to technical operators.
- Operator identifiers and passwords are communicated to technical operators.

This installation is not included in the evaluation perimeter insofar as it concerns the entire platform and not only the boot.

EA4. Physical protection

Physical access to the machine on which D3S is hosted, is supposed to be controlled in order to prevent any alteration through this.
In case where the D3S is made available as an online service, this assumption covers the system administrators in charge of maintaining the operational condition of the servers hosting the service.

EA5. Source of time

The accuracy of the clock against which D3S synchronizes to date logged or archived events must be less than 1 second compared to UTC time. This time source is assumed to be reliable.

EA6. Operations witness

It is assumed that the authority carries out regular checks on the proper functioning of the approved platforms. In particular, this authority itself generates operations, called “witness operations” upstream of the captor for the sole purpose of noting the presence of associated digital evidences in the SAFE.
The purpose of this measure is to detect any attempt by the operator to bypass the recording of digital evidences of operations by the platform (diversion of flows, setting up of a parallel site, etc.).

EA7. Trusted administrators

It is assumed that the administrator from the authority or designated by it can be trusted.

EA8. Trusted technical operators

It is assumed that the technical operators personnel that have access to the service or to the physical platform hosting it are trusted, competent and have received an adequate training on information system security.

EA9. Decryption key

The (private) decryption key specific for a gaming operator that is used by **d3sc** must be kept confidential by the d3sc user agent and used only by authority who has received access rights to this product. In particular, it must in no case be communicated to the gaming operator. This key is fully controlled by the issuing authority. Only agents with control and audit power scan have access to this key, which product users must make sure to keep in secure conditions.

3.3. Assets to protect

A1. D3S configuration data

This data covers in particular user profiles and the (public) encryption key. Only **D3S** administrators can modify the **D3S** configuration.

This asset is protected in integrity.

A2. Digital evidences

D3S must ensure two main properties relating to the security of the digital evidences it keeps:

- On the one hand, only authorized profiles have access to the deposited items (confidentiality of the contents of the trace)
- Any alteration of the traces is detectable (integrity of deposits)
- On the other hand, we must be able to check the integrity and completeness of the deposit proofs. Integrity relates to individual deposit proof, while completeness refers to integrity of the sequence of this deposit proofs (chaining). No one should be able to delete, modify or insert a digital evidence without it being detectable.

D3S ARJEL Client (d3sc) must ensure two main properties relating to the security of the digital evidences:

- Receive the deposit proofs by a secure channel protected in integrity and confidentiality against any other user of the TOE[1].
- Detect and report any alteration in the integrity and completeness of the deposit proofs received. Integrity relates to the individual deposit proof, while completeness refers to the integrity of the sequence of this deposit proofs (chaining).

This asset is protected in confidentiality and integrity. The integrity protection covers both the evidences individually, and the chain of evidences as a whole

3.4. Threats considered

T1 Deposit of dummy traces

An attacker makes deposits in **D3S** other than through the authorized captor. The objective may be to saturate the storage space for traces in order to mask subsequent fraudulent operations (which would not be traced). Likewise, these deposits can themselves serve to simulate non-existent activity.

T2 Dummy trace injections

An attacker directly adds or modifies the content of the storage space. This is the same attack as before, but carried out on the storage space rather than on the repository interface.

T3 Data Theft

An attacker accesses the storage space and extracts data relating to the operator's activity there.

T4 Erasing digital evidence

An attacker accesses the storage space and deletes records there.

T5 Configuration modification

An unauthorized person (i.e. other than a D3S administrator) changes the configuration of the D3S. This attack is essentially a prerequisite for the realization of the other threats.

Technically, the alternation of the configuration amounts to an attacker taking control of the SAFE: if the attacker can modify the configuration at will, he is likely to modify the critical parameters of the SAFE.

T6 Man in the middle

An attacker tries to insert himself into the flow of commands and data transferred between the **d3sc** tool and the D3S safe server, in order to get access to its content or else to alter the transmitted data.

T7 Compromise of access

An attacker who obtained a copy of the **d3sc** tool tries to use it to obtain data from the D3S safe server, without having access to the (private) decryption key of the *d3sc user agent*.

T8 Compromise of evidence

An attacker tries to modify or delete data in storage space of the D3S safe server without being identified by the **d3sc** tool when the Authority checks the corresponding evidence.

---

[1] *in the implementation, a transport archive is used for the transfer of deposit proofs*

4. Security functions

4.1. SF1 Strong user authentication

D3S strongly authenticates all users so as to ensure the integrity of this configuration and the authenticity of the repositories (only a *"depositor"* profile can add a trace in D3S, in this case, taking into account the assumptions about the initialization of the platform, only the captor is authorized to make deposits). Anyone (or system) wishing to access the digital SAFE is identified and strongly authenticated by certificate.

Finally, **D3S** secures the flows between the client and itself by implementing the standard TLS protocol. The implementation of TLS / SSL by the **D3S** server ensures:

- Strong mutual authentication of the parties (D3S server and a caller) by certificate
- Control of flow integrity
- Confidentiality of the data exchanged

As client of **D3S**, **D3S ARJEL Client (d3sc)** uses the authentication method specified above when accessing the D3S.

4.2. SF2 Digital evidence chaining

Any deletion, modification or insertion of a digital evidence must be detectable. This function therefore ensures the chaining of the different deposited digital evidences: each digital evidence is cryptographically linked to the digital evidence which precedes it chronologically via the chaining of the deposit proofs associated with the digital evidences.
This chaining ensures the following properties:

- On the one hand, the deposit proof is complete; any change in deposit proof is detectable.
- On the other hand, any modification of the sequence of deposit proof (deletion, insertion, displacement or addition) is detectable.

Note: assuming that the attacker has sufficient access and rights to the storage space, he can nevertheless delete the traces and associated proofs from "the end of the chain", or even delete all (a blank storage space is intact and properly chained). This attack is part of the risks assumed insofar as several elements contribute to lessening its effects and the possibility of its realization.

- First the attacker has to have the necessary rights and access.
- Then, the context of the use of the product implies a large volume of operations, and any intervention of this type on the storage space without it breaking the chaining (it is necessary to delete the last digital evidence before the following digital evidence does not registered by the platform) is complex to implement. The solution consisting in stopping the platform or interrupting the flow upstream of the captor is detectable at the date of the digital evidences.
- Finally, such manipulation is likely to erase a *"control operation"*, which will then be detected (see the hypothesis on control operations).

4.3. SF3 Encryption and sealing of deposits (traces)

D3S encrypts all the data deposited (traces) in a given safe with a public encryption key defined in the configuration. This encrypted trace is returned as is when exported by an authorized user. The decryption of the trace can only be done on the local station of the latter, provided that it has the appropriate private key.

In addition, the integrity of the traces deposited is ensured by an electronic signature mechanism (sealing). So:

- A deposit proof is generated and signed when the trace is placed in the safe (deposit)
- The signature of this proof is validated when the trace is returned (audit / withdrawal)

This proof can be returned to the user or to the external module making the deposit.

4.4. SF4 Decryption and validation of deposits

D3S ANJ Client (d3sc) decrypts the transport archives on the local station of an employee of the Online Games Regulatory Authority (ANJ), provided that he has the private key (either in an HSM or in a software store).
The integrity of the traces deposited is ensured by the validation of electronic signature (sealing) of the deposit proof which is generated and signed when a trace (deposit) is placed in the SAFE in **D3S**.

4.5. SF5 Signature of the configuration

The configuration of the SAFE (**D3S**) is described in a signed file. This file contains the access rights for each user of the system. The signature of this file is verified on the first request for authorization to deposit.

5. Technical supplements

5.1. Algorithms used

D3S offers secure encryption and decryption mechanisms using symmetrical and asymmetric algorithms respecting cryptographic norms and standards.

Signature

D3S implements the signature formats are as follows:

- Signature format for the trace: XAdES
- Hash algorithm: SHA256
- Signature algorithm: RSA with SHA256

Encryption

The encryption mechanisms are as follows:

- Encrypted format for the trace: XMLEnc
- Symmetric encryption algorithm: AES
- Asymmetric encryption algorithm: RSA with OAEP padding.

6. Coverage of the threats by the security functions

D3S threats

	Strong user authentication	Digital evidence chaining	Encryption and sealing of deposits	Signature of the configuration
Deposit of dummy traces	X			X
Dummy trace injections		X	X	
Data Theft			X	

Erasing digital evidence		X		
Configuration modification				X

D3S ANJ Client threats

	Strong user authentication	Digital evidence chaining	Decryption and validation of deposits
Man in the middle	X		
Compromise of evidence		X	X
Compromise of access			X