

Pouzdanost dokumenata pohranjenih unutar Europske digitalne lisnice

ljubimko.simicic@axians.hr

Što je Europska digitalna lisnica?

- Europska digitalna lisnica odgovara na izazove **identifikacije** korisnika,
- Europska digitalna lisnica omogućuje **pohranu** digitalnih dokumenata,
- Europska digitalna lisnica omogućuje **dijeljenje** digitalnih dokumenata,
- Europska digitalna lisnica omogućuje **pristup** servisima,
- Europska digitalna lisnica omogućuje digitalno **potpisivanje**.

Koje su prednosti uporabe Europske digitalne lisnice?

- Olakšan pristup do javnih i privatnih servisa,
- Osobni podaci su zaštićeni i pod kontrolom korisnika,
- Jednostavnija registracija korisnika prema servisima,
- Otežano je lažno predstavljanje korisnika prema servisima,
- Primijenjena su najnovija sigurnosna rješenja.

Što je bit svega?

- Autentikacija...



"On the Internet, nobody knows you're a dog."

O čemu ovisi pouzdanost Europske digitalne lisnice?

- Pouzdanost i uporaba Europske digitalne lisnice ovisi o pouzdanosti dokumenata pohranjenih unutar Europske digitalne lisnice,
- Proces stvaranja dokumenata za pohranu unutar Europske digitalne lisnice mora biti usklađen sa svim relevantnim EU i međunarodnim sigurnosnim standardima i preporukama,
- Tijekom procesa izrade dokumenata potrebno je uporabiti sklopovska i programska rješenja koja su usklađena sa svim relevantnim međunarodnim sigurnosnim standardima.

Koje su osnovne pretpostavke za izradu dokumenata?

- Europska digitalna lisnica izrađena je po svim sigurnosnim standardima,
- Dokumenti se na siguran način pohranjuju unutar Europske digitalne lisnice,
- Dokumenti se izrađuju, proizvode od strane ovlaštene institucije,
- Izrada dokumenta mora biti urađena uporabom sigurnosno provjerenih, (certificiranih) programskih i sklopovskih podsustava,
- Ovlaštena institucija jamči za ispravnost i cjelovitost podataka koji se upisuju unutar dokumenata.

Kako otežati lažno predstavljanje?

- Uporabom digitalnih tehnologija i certificiranih rješenja otežano je tako zvano „krivotvorenje” dokumenata,
- Ovdje bi se trebao uporabiti pojam lažnih dokumenata,
- Dokumenti su tehnički ispravni te izrađeni po svim sigurnosnim pravilima ali su podaci koji se koriste prilikom izrade neistiniti.

Kako osigurati sigurnost podataka?

- Ovdje se dakle radi o sigurnosti podataka prije izrade dokumenta,
- Podaci moraju biti prikupljeni i obrađivani uporabom procesa i procedura usklađenih s poslovnim politikama vlasnika podataka te relevantnim nacionalnim i EU regulativama,
- Nakon svega postoji problem „socijalnog inženjeringa” i problem „ljudskog faktora”,
- Potrebna je trajna edukacija i osviještenost djelatnika koji obavljaju prikupljanjem podataka, obradu podataka te izradu dokumenta.

Osnovni proces izrade digitalnih dokumenata?

- Iz postojećih poslovnih sustava dohvate se potrebni podaci,
- Podaci se grupiraju i oblikuju prema zahtjevima standarda koji opisuje određeni digitalni dokument,
- Podaci se digitalno potpisuju na siguran i pouzdan način,
- Tako potpisani podaci pohranjuju se u digitalni oblik dokumenta,
- Dokument je spreman za pohranu u Europsku digitalnu lisnicu.

Kako zaštititi podatke?

Osigurati tajnost podataka - šifriranje

- Unutar aplikacija,
- Unutar sustava pohrane,
- Unutar baza podataka,
- Unutar operacijskih sustava,
- Unutar virtualnih podsustava,
- Unutar podsustava u oblaku,
- Tijekom uporabe računalnih mreža.

Kako zaštititi podatke?

Analiza podataka ...

- Procjena rizika (ranjivosti i prijetnje),
- Sigurnost infrastrukture i podataka,
- Potrebna ili željena sukladnost s relevantnim standardima.

Kako zaštititi podatke?

Potrebne ili željene zaštite podataka ...

- Zaštita aplikacija i razvojnih alata/biblioteka,
- Zaštita uređaja koji se uporabljaju kod pristupa podacima,
- Zaštita od neželjenih korisnika te neželjene aktivnosti,
- Zaštita od eventualnih pristupa sustava AI,
- Zaštita od prikupljanja podataka za kasniju uporabu (QC).

Kako zaštititi podatke?

Upravljanje pristupima do podataka ...

- Razvoj politika pristupa korisnika baziran na ulogama, lokacijama te ostalim značajkama korisnika,
- Razvoj politika pristupa ovlaštenim administratorima baziran na resursima koje održavaju,
- Razvoj politika pristupa baziran na sadržaju podataka.

Kako zaštititi podatke?

Praćenje podataka ...

- Praćenje uporabe podataka unutar baza podataka,
- Praćenje uporabe podataka unutar aplikacija,
- Praćenje uporabe datoteka operacijskog sustava,
- Prepoznavanje prijetnji zloporabe podataka,
- Upravljanje uporabom podataka.

Kako zaštititi podatke?

Sigurnost aplikacija koje rade s podacima ...

- Postavke sigurnosti klijenata koji obrađuju podatke,
- Sigurnost programskih alata i biblioteka programa za obradu podataka,
- Zaštita pristupa do aplikacija:
 - Aplikacijski vatrozid,
 - Vatrozid računalne mreže,
 - Zaštita od automatiziranih napada,
 - Zaštita od zagušenja resursa.

Zaključak

- Tijekom procesa izrade dokumenata potrebno je uporabiti sklopovska i programska rješenja koja su usklađena sa svim relevantnim međunarodnim sigurnosnim standardima.
- Izrada dokumenata mora biti urađena uporabom sigurnosno provjerenih, (certificiranih) programskih i sklopovskih podsustava,
- Ovlaštena institucija jamči za ispravnost i cjelovitost podataka koji se upisuju unutar dokumenata.

THALES

... primjerice

Thales CipherTrust Data Security Platform

Data Protection | Key Management & Policies |
Activity Monitoring | Risk Management & Analytics



File-level
Encryption and
Access Control



Database
Encryption



Application Data
Protection



Tokenization



Key
Management



Secrets
Management



Unstructured
Data Discovery
& Classification



Structured
Data Discovery
& Classification



Data Activity
Monitoring



Data Risk
Management



Sensitive Data
Management



Compliance
Management

Thales Luna HSM

Hardware Security Modules | Highest level Root of Trust |
Future-Proof Quantum Protection



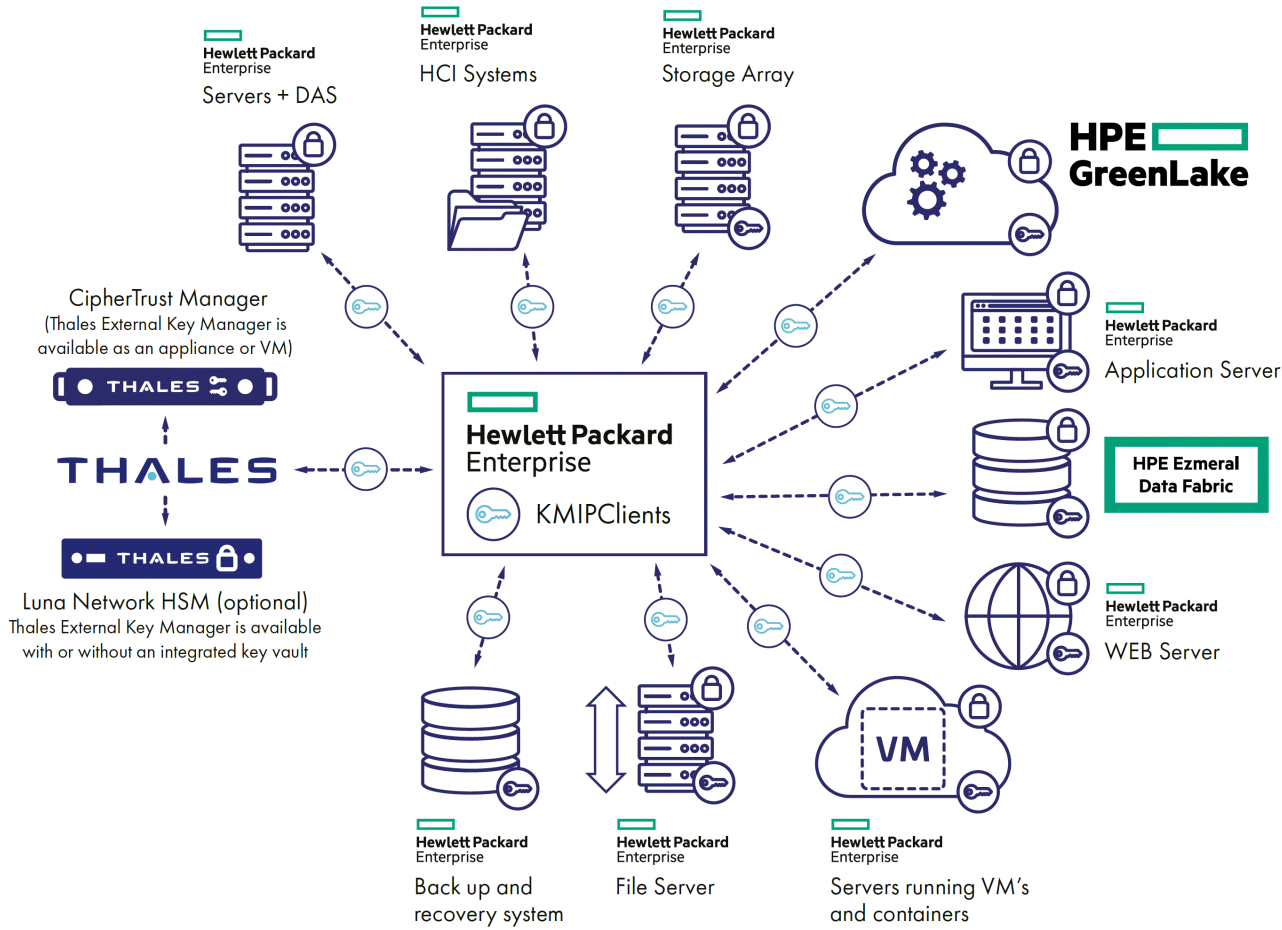
HPE

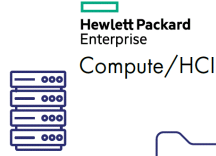
HPE ProLiant Compute

Trusted Performance at Scale | AI & Data-Driven
Optimization | Sustainable & Cost-Efficient



... primjerice





Hewlett Packard Enterprise File / App / Web Servers

... primjerice

THALES

HPE GreenLake Flex (aas) Solutions
Preintegrated with HPE (GreenLake, Compute, Storage, etc.) and Multi-cloud (Hyperscalers)



Centralized Enterprise Key Management



Multi- and Hybrid-Cloud Key Management



Hardware Security Module (HSM)



Secrets Management



Encryption



Tokenization



HPE GreenLake

Edge-to-cloud platform



Hewlett Packard Enterprise Storage



Hewlett Packard Enterprise Databases



Hewlett Packard Enterprise Back up and Restore



Hewlett Packard Enterprise Ezmeral Data Fabric

Hvala

ljubimko.simicic@axians.hr