

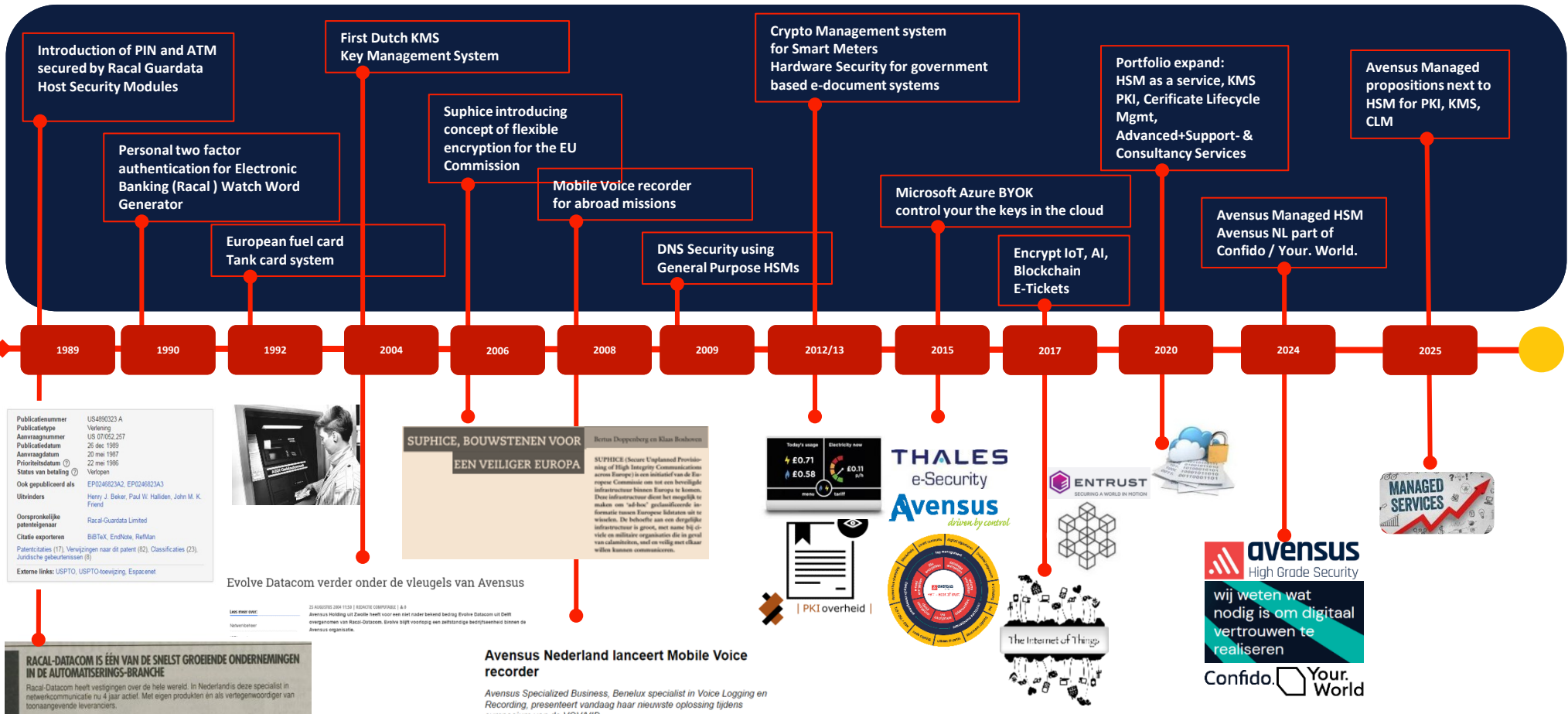
Avensus Nederland B.V.
Your certified cryptography partner

Yivi Meetup
17 April 2026

Agenda

1. Introduction to Avensus (3 Slides)
2. What is an HSM and why would you use it (4 Slides)
3. Why is this important ? (5 Slides)
4. Closing & Q&A

Avensus High Grade Security, shaping an industry



Publicatienummer: US4980323 A
 Publicatietype: Verleening
 Aanvraagnummer: US 07/052,257
 Publicatiedatum: 26 dec. 1989
 Aanvraagdatum: 20 mei 1987
 Prioriteitsdatum: 22 mei 1986
 Status van betaling: Verlopen
 Ook gepubliceerd als: EPI0246823A2, EPI0246823A3
 Uitvinders: Henry J. Baker, Paul W. Halliden, John M. K. Friend
 Oorspronkelijke patenteigenaar: Racal-Guardata Limited
 Citatie exporteren: BIBeTeX, EndNote, RefMan
 Patentcites (17): Verwijzingen naar dit patent (82), Classificaties (23), Juridische gebeurtenissen (8)
 Externe links: USPTO, USPTO-toewijzing, Espacenet



SUPHICE, BOUWSTENEN VOOR EEN VEILIGER EUROPA

Bertus Deppenbergh en Klaus Boshuizen

SUPHICE (Secure Unplanned Provisioning of High Integrity Communications across Europe) is een initiatief van de Europese Commissie om tot een beveiligde infrastructuur binnen Europa te komen. Deze infrastructuur dient het mogelijk te maken om 'ad-hoc' gesloten-netwerken te bouwen. De behoeften aan een dergelijke infrastructuur is groot, met name bij officiële en militaire organisaties die in geval van calamiteiten, veel en veilig met elkaar willen, kunnen communiceren.



THALES e-Security
Avensus
 driven by control

ENTRUST
 SECURING A WORLD IN MOTION



MANAGED SERVICES

Evolve Datacom verder onder de vleugels van Avensus

20 OKTOBER 2004 11:50 | REDACTIE COMPAGNIE | A & A
 Avensus Holding uit Zwolle heeft voor een jaar een beheerbedrijf Envisia Datacom uit Delft overgenomen van Raza-Qadom. Envisia blijft voortoppg een zelfstandig bedrijfsmiddel binnen de Avensus organisatie.

RACAL-DATACOM IS EEN VAN DE SNELST GROEIENDE ONDERNEMINGEN IN DE AUTOMATISERINGS-BRANCHE

Racal Datacom heeft vestigingen over de hele wereld. In Nederland is deze specialist in netwerkcommunicatie nu 4 jaar actief. Met eigen producten en als vertegenwoordiger van toonaangevende leveranciers.

Avensus Nederland lanceert Mobile Voice recorder

Avensus Specialized Business, Benelux specialist in Voice Logging en Recording, presenteert vandaag haar nieuwste oplossing tijdens symposium van de VOVVID

Amsterdam, NL, 30 oktober 2008

General Electric's GE Information Services has signed a co-operative marketing agreement with Racal-Guardata Ltd to sell a UK-developed hardware security system with its worldwide network services. The system, which Racal developed initially for GE's Money Transfer System, is pre-erited by Racal-Guardata as a predecessor to the forthcoming Super Smart Card and competitor to the existing ones, and is designed to prevent criminal tampering with electronic funds transfer over GE's network. Racal will sell the system separately in the US through a new company based in Orange County, California. Racal-Guardata Inc, and says it is talking to banks and network operators worldwide about the system. It consists of a plug-in tamper-resistant Personal Computer board or a fault-tolerant security module peripheral for mainframes - dubbed Watch-word and launched last July as an access control device, and is used as a personal identification device to authorise a transaction. It is based on the ANSI data encryption algorithm standard. The system costs around \$2,500 for a Personal Computer package and \$10,000 to \$30,000 for a mainframe package. Managing director of GE's International Banking and Financial Services, Jamie Graham, said that network costs to the user will be reduced using the security system because processing is distributed to the back office processor rather than in the network.

What Avenusus High Grade Security stands for



WHO WE ARE

Avenusus High Grade Security is the trusted expert in encryption and key management in the Benelux. Our specialists are certified experts on cryptography, tooling and everything related.



WHAT WE DO

Avenusus High Grade Security secures the world's most sensitive information from financial transactions to intellectual property.



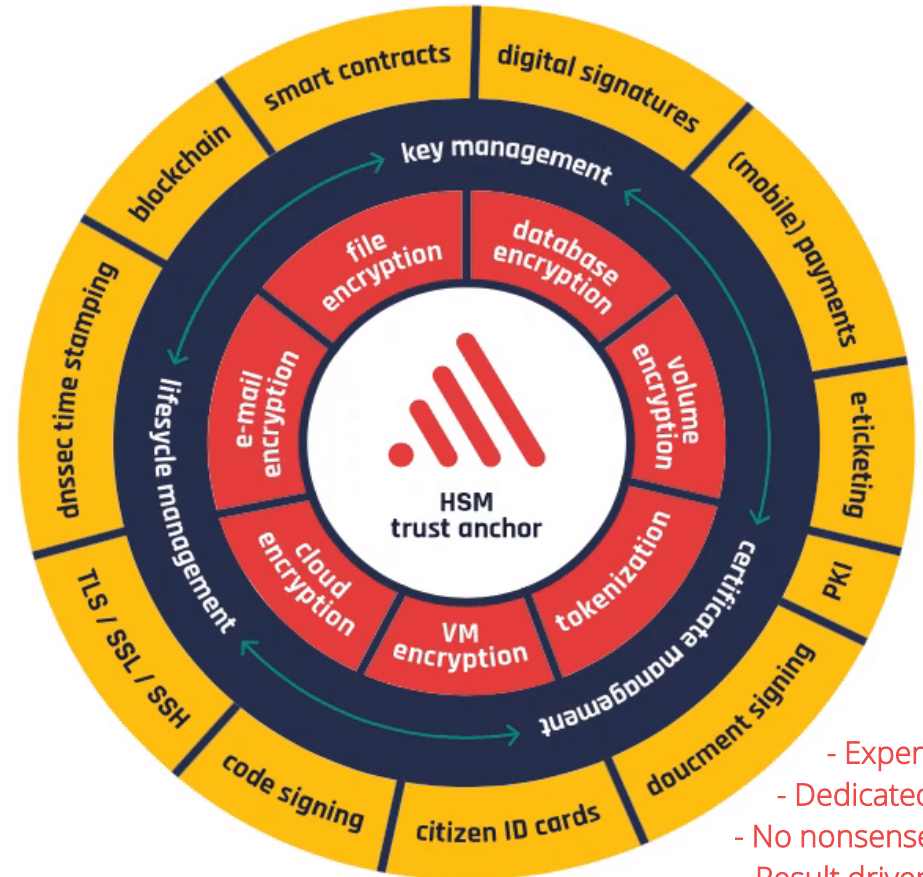
WHAT WE BELIEVE IN

Hardware provides the highest security level; Our motto is "Encrypt all and manage the keys yourself".



WHAT WE WANT TO ACHIEVE

Be your end-to-end partner in data protection: from your HSM's, encryption, certificate lifecycle- & central key management by building digital trust; Cloud trust is not proven until you can touch it.



Avensu Advanced Support Services

Note: Avensu Advanced Support today for Entrust nShield and Thales PayShield & Luna HSMs.

Advanced

- Office Hours 8.30-17.00
- 1st – 3rd line via Avensu
- 4hrs response time
- Next day HW replace
- On-site replace HGS
- Incl. Vendor Support

Advanced Plus

- 24*7 hours coverage
- 1st – 3rd line via Avensu
- 4hrs response time
- 4hrs HW replace
- On-site replace HGS
- Incl. Vendor Support

Advanced

- Vendor Support
- 1st line Avensu->Vendor
- Office Hours 8.30-17.00
- Updates + M&S

Advanced Plus

- Vendor Support
- 1st line Avensu->Vendor
- 24*7 hours coverage
- Updates + M&S

Managed Services

Under construction: Avensu Managed PKI, CLM, KMS, CSP

Avensu Managed HSM

- HSM as a Service
- Serviced by Avensu
- (NL) Private cloud (DC Customer or HGS)
- Access to HSM
- Monitoring of HSM
- 24*7 hours coverage
- Self or Fully managed
- X hrs response time
- Incl. Vendor Support

- Avensu / Vendor Support
- Change Mgmt Avensu
- 24*7 hours coverage
- Updates + M&S

Consulting Services

Strategic Consultancy

Consultancy & Engineering

Service Delivery Management

Technical Advisory Services

Training services

Projects & Implementation

Agenda

1. Introduction to Avensus (3 Slides)
2. What is an HSM and why would you use it (4 Slides)
3. Why is this important ? (5 Slides)
4. Closing & Q&A

What does an HSM look like ?

- Entrust's next-generation hardware security module
- For organizations seeking a world-class HSM platform in a range of network-attached, PCIe and USB models
- **nShield 5s** and **nShield 5c**
 - High performance with crypto-agile architecture – future-proof technology
 - FPGA design enables future in situ firmware upgrade to PQ cryptography
- **nShield 5e** (*coming soon*)
 - Portable HSM usage with PC/laptop and offline Root CA use cases



nShield 5c & 10g



nShield 5s

A common architecture across all form factors enables mixed pool of HSMs

Benefits of using HSM's: Key Protection !

- **Lack of due care of sensitive material creates risks**
 - **Keys in software are much easier to steal**
 - Sensitive key data is in server memory during operations
 - Core dumps can reveal sensitive data
 - Stored key data is only as secure as the passphrase (if any) protecting it
 - **Storing keys in hardware is not only best practice but also often mandated**
 - **Improper/inadequate storage or use puts trust at risk**
- **HSMs provide a secure environment for key generation and usage**
 - **are Random Number Generator**
 - Key generation use the onboard tRNG as a source of strong entropy
 - **Access to keys can be further restricted using card sets and/or passphrases**
- **Critical application code can run protected in a Secure Execution Environments, within the HSM**
 - **Custom applications run in a secured/sandboxed container**

Benefits of using HSM's: Performance !

- **Optimized crypto hardware**
 - **FPGA programmable, accelerated algorithms**
 - **Multiple tenants, cryptographically separating keys in hardware make contexts switching much faster**
 - **Certified storage mechanisms allows for secure offloading of non-active keys**

Available Models and Performance

nShield 5c Models	Base	High
RSA signing performance (tps) for NIST recommended key lengths		
2048 bit	670	13,614
4096 bit	135	2,200
8192 bit	19	309
ECC prime curve signing performance (tps) for NIST recommended key lengths		
256 bit	2,085	21,826
512 bit	1010	16,164
Key generation (keys/sec)		
RSA 2048 bit	7	23
ECDSA P-256 bit	1,040	3,580
ECDSA P-521 bit	518	2,724
Key agreement performance (transactions/sec)		
ECDH P-256 bit	2,085	21,436

Benefits of using HSM's: Compliance !

- **FIPS 140-2 Level 3 Certified**

- <https://www.entrust.com/digital-security/hsm/solutions/compliance/certifications/fips-140-2>

- **Common Criteria Certified**

- <https://www.entrust.com/digital-security/hsm/solutions/compliance/certifications/common-criteria>

- **European Commission eIDAS Compliance**

- <https://www.entrust.com/digital-security/hsm/solutions/compliance/emea/eidas>

- **Payment Card Industry (PCI) Data Security Standard (DSS) Compliance**

- <https://www.entrust.com/digital-security/hsm/solutions/compliance/global/pci-dss>

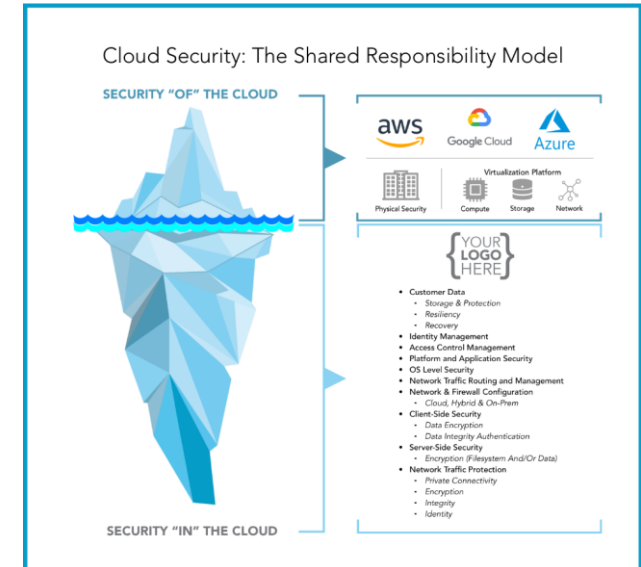


Agenda

1. Introduction to Avensus (3 Slides)
2. What is an HSM and why would you use it (4 Slides)
3. Why is this important ? (5 Slides)
4. Closing & Q&A

Awareness of Digital Sovereignty & Shared Responsibility

Country/bloc	Overall approach to digital sovereignty	Approach to personal data	Approach to non-personal data
U.S.	Does not adopt laws on digital sovereignty. Advocated by Big Tech, unregulated. Big Tech plays a significant role. <i>Leave it to Big-Tech</i>	No unified approach to protection of personal data at the federal level. States regulate. TSPs (US and overseas) Act as data controllers. Authorities to demand access to data held by US companies overseas. <i>All your datas belong to US</i>	Free flow of non-personal data. <i>All your datas belong to US</i>
China	Promotes a government-led approach to digital sovereignty. Big Tech has to comply with government requirements to protect data on the internet. <i>We decide what's Best for you</i>	Personal Information Protection Law (PIPL) has similarities with the EU's General Data Protection Regulation. Extraterritoriality principle. Data localization requirements of critical information infrastructure operators. Additional requirements e.g. local storage of personal information by critical information infrastructure operators. <i>All your datas belong to US</i>	Non-personal data classified according to national security. Public information security law and 2017 Cybersecurity Law with security assessment before data is transferred abroad. <i>All your datas belong to US</i>
E.U.	Third way between the US (unregulated surveillance capitalism) and Chinese (surveillance capitalism) models with a strong focus on individual rights. <i>Meh</i>	Protection of personal data is a fundamental right with mandatory requirements under the GDPR for processing personal data. Externalization of GDPR to non-EU entities. States the EU can only access personal data if it is necessary for law enforcement. Restrictions on transfers of personal data, and requirements on how personal data is treated once it has left the EU/EEA. <i>Your data Belongs to You</i>	Free flow of non-personal data. Third world countries access personal data and mechanisms to ensure availability. <i>Your data STILL Belongs to You</i>



Shared Responsibility relevance!
Cloud Service Providers (CSP's) provide a lot of capabilities and ease of use. For cloud cryptography CSP's rely on cloud native encryption, owned by CSP, used by customer.



Need I Say More ?



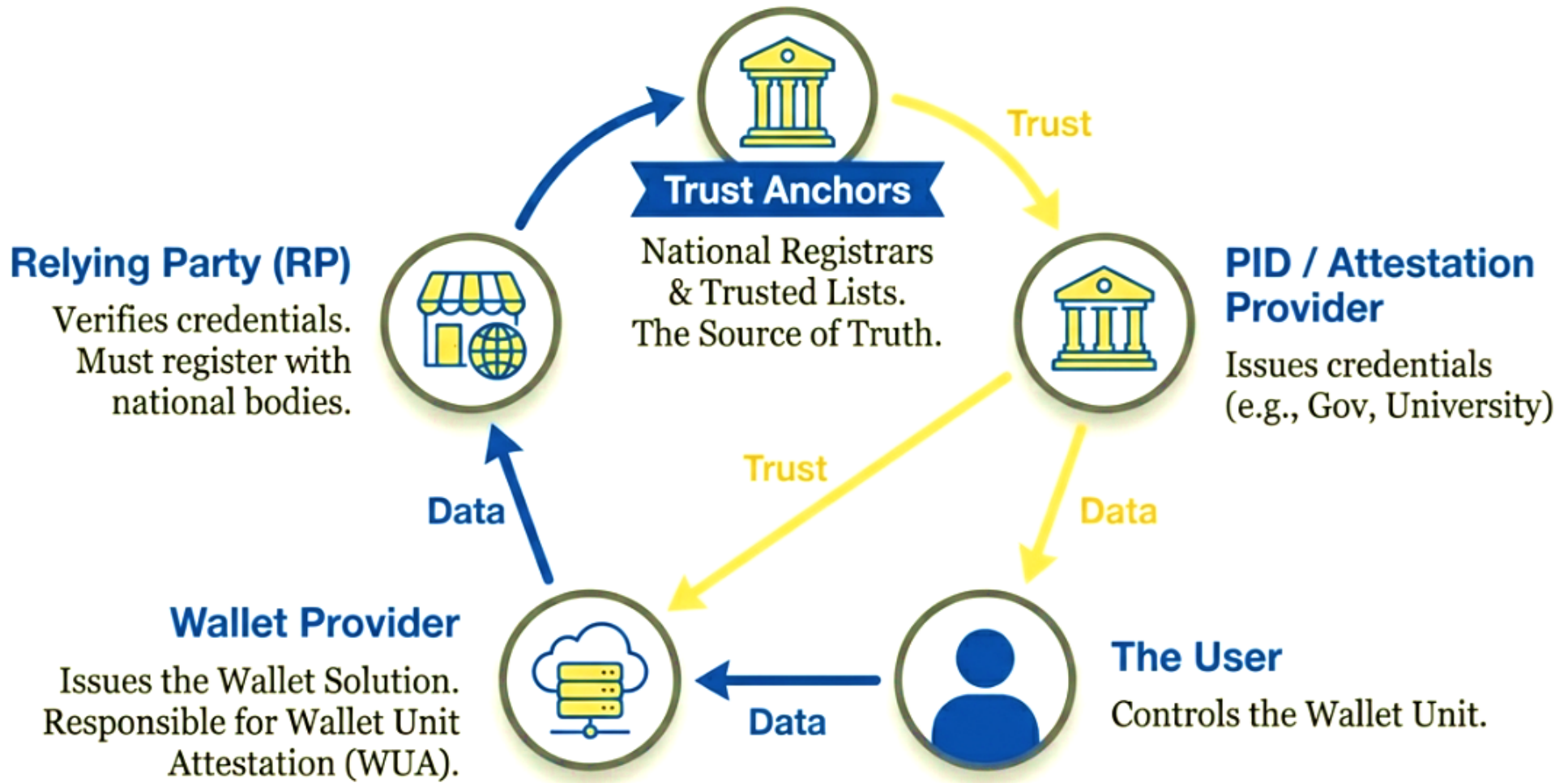
Home > NDS nieuws > Nederland moet zelf baas worden over digitale toekomst

Nederland moet zelf baas worden over digitale toekomst

Digitale weerbaarheid 3 april 2026



The Ecosystem: A Chain of Trust

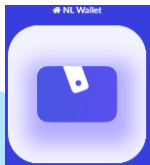


EUDI Wallet implications

The requirement for "sole control" over cryptographic keys is established by **Regulation (EU) 2024/1183** (commonly known as **eIDAS 2.0**), which amends the original eIDAS Regulation (EU) No 910/2014 1, 2. The law mandates that *every EU citizen has the right to a digital identity that is under their **sole control**, which specifically includes maintaining **exclusive** authority over the sensitive cryptographic material, such as private keys, used to sign and authenticate data* 3, 4.

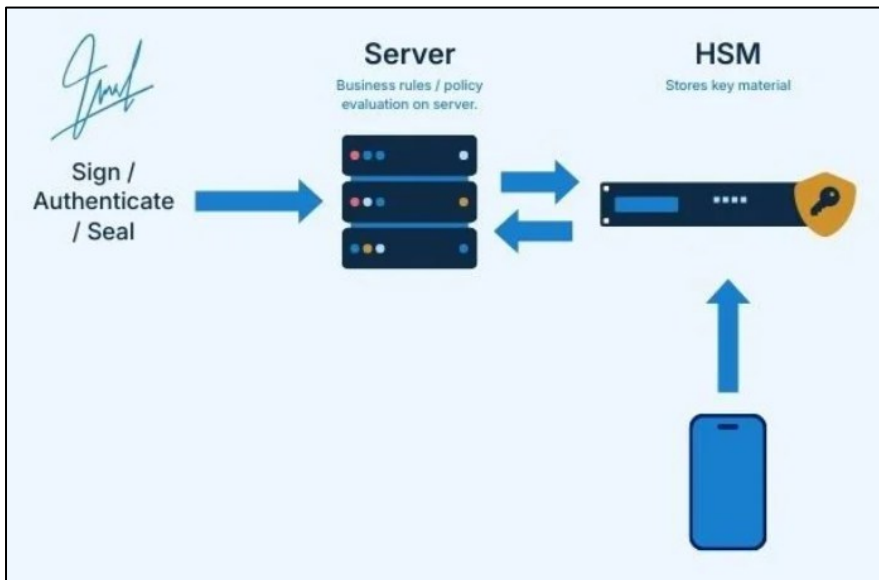
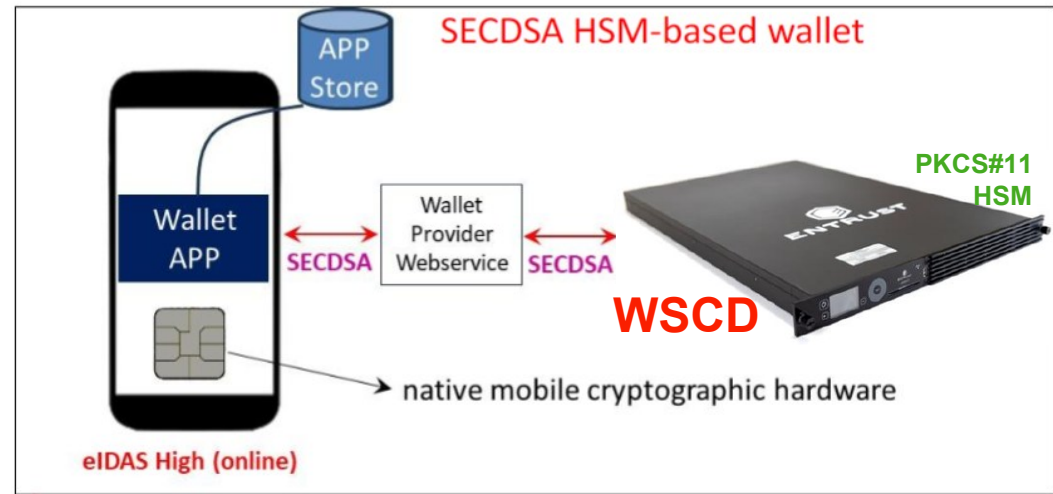
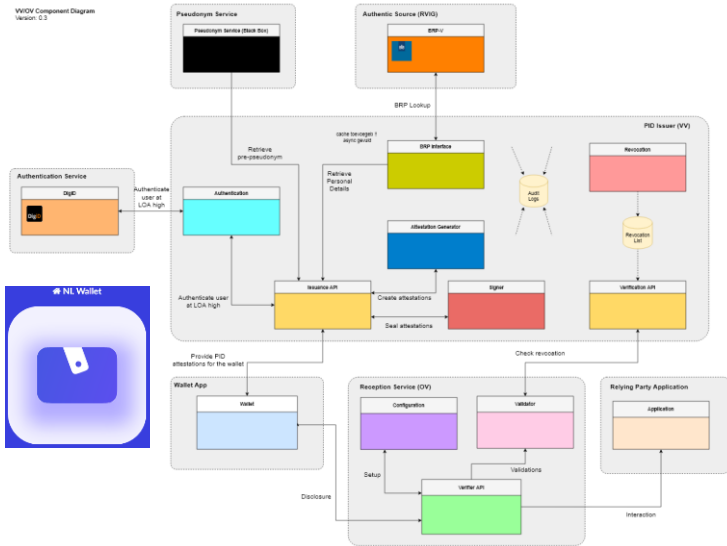
This mandate has profound implications for the technical architecture of the European Digital Identity (EUDI) Wallet:

1. Mandatory Secure Hardware (WSCD/QSCD)
2. Dual-Layer Authentication
3. Device Binding
4. Constraints on Migration and Backup
5. Unobservability and Unlinkability



Apple App Attest / Google Play Integrity
Online services that provide security features for iOS and Android. App Attest and Play Integrity are used to prove that an app instance is genuine and to prove that **the Wallet-App private keys are stored securely.**

"Simple" architectures using an HSM



Agenda

1. Introduction to Avensus (3 Slides)
2. What is an HSM and why would you use it (4 Slides)
3. Why is this important ? (5 Slides)
4. Closing & Q&A



What Avenusus High Grade Security stands for



WHO WE ARE

Avenusus High Grade Security is the trusted expert in encryption and key management in the Benelux. Our specialists are certified experts on cryptography, tooling and everything related.



WHAT WE DO

Avenusus High Grade Security secures the world's most sensitive information from financial transactions to intellectual property.



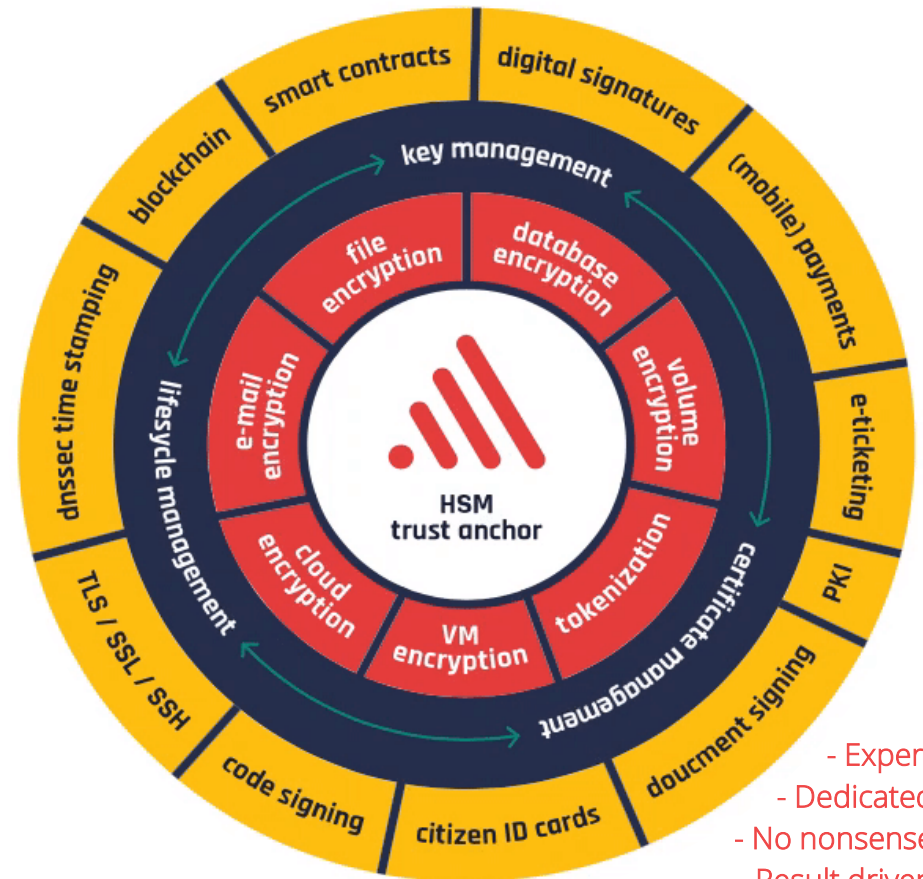
WHAT WE BELIEVE IN

Hardware provides the highest security level; Our motto is "Encrypt all and manage the keys yourself".



WHAT WE WANT TO ACHIEVE

Be your end-to-end partner in data protection: from your HSM's, encryption, certificate lifecycle- & central key management by building digital trust; Cloud trust is not proven until you can touch it.



Avensus Nederland B.V.
Your certified cryptography partner

Yivi Meetup
17 April 2026