Post-Quantum

Cryptography Conference

Cryptographic Discovery and Inventory: The Hidden Foundation for Enterprise Security

Alexander Löw
CEO at Data-Warehouse

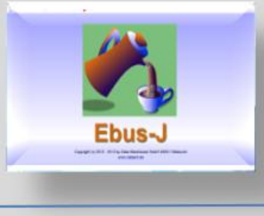
October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKIC PQC Conference

Cryptographic discovery, inventory, risk assessment, Cybersecurity Challenges, Compliance, Software Supply Chain Control and need for crypto agility

Data-Warehouse GmbH
Cybersecurity

Data Warehouse GmbH

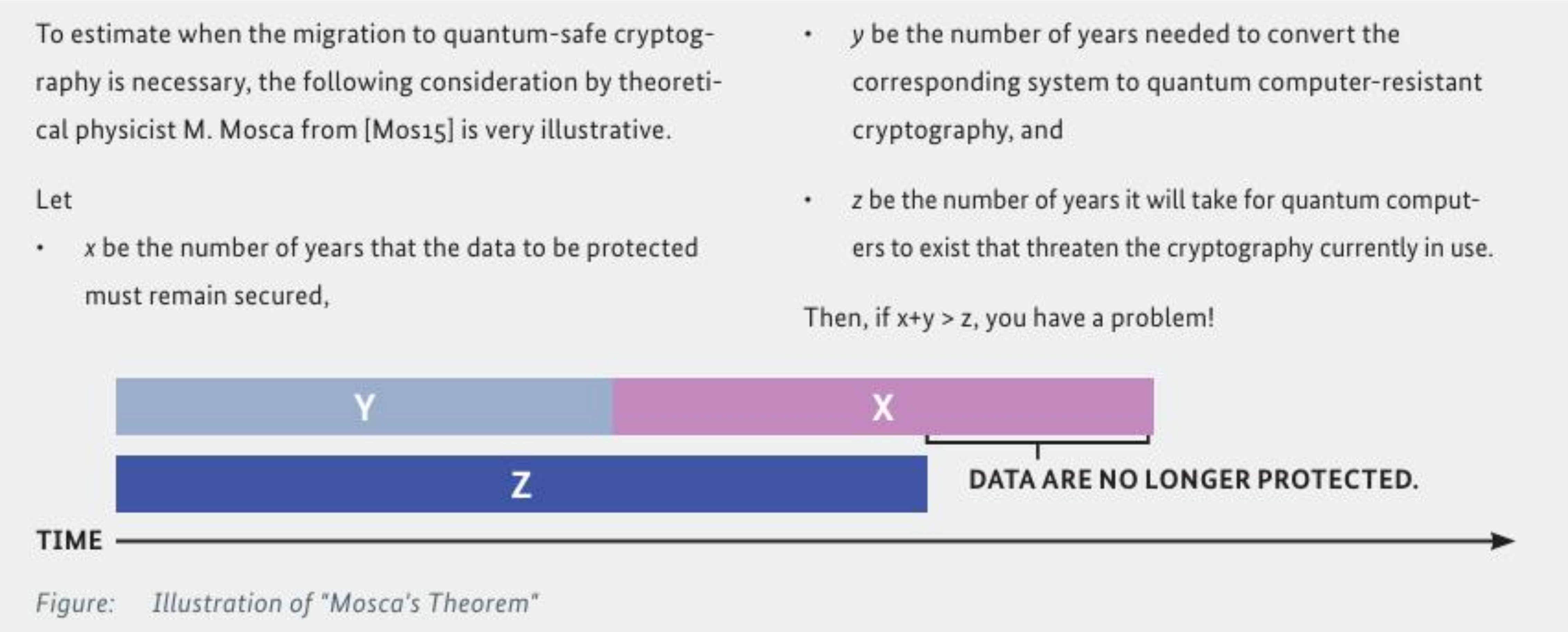
Our portfolio		Our products Made in Germany	Our customers
Software development	•Cybersecurity •Individual & SME multiple branch and production solutions •Networking implementation and Communication solutions •Low Code Universal Software development platform (EBUS –J) •Consulting, Support, GDPR Consulting (GDPR) •Project management		DER PARITÄTISCHE BAYERN Audi Bärwurzerei Hieke Zwiesel SIEMENS handicap international humanité & inclusion KINDER SCHUTZ MÜNCHEN
+ Information management	•Enterprise Solutions, Data Center solutions •Central information mangement systems, Logistics optimisation, PLM/PDM, Supply chain optimisation •Distributed database systems •Social collaboration, messaging (tixxle) •Master data management & logistics (IQIMS) •(High) secure software development •Mobile, Cloud and web solutions	IQIMS SPOT Platform Interface Plan Do Check Act IQ IMS	Deutsche Post Bundeswehr Eurofighter Typhoon AIRBUS DEFENCE & SPACE O2 Deutsche Börse Group Bundesheer OCCAR ESG EnBW DB BAHN
+ (IT & ID) Security	•Implementation strategy of complex products •I(T-)Security concepts for high secure areas •Cyber security strategies, security research •Development of national standards •Online trainings, awareness, pentesting •Implementation of (national) CA and PKI •Identity Management und Privileged Identities •P-Cert		BMW Eurofighter Typhoon BNotK BUNDESNOTARKAMMER secunet TMS AIRBUS DEFENCE & SPACE EVG HUK-COBURG

ISO 9001 | ISO 27001 | Aero Excellence Certified

Governance /Compliance

- US approach
  - Inventorisation of all cryptographic items until 2030
  - NIST: Post Quantum Migration projects
  - CISA: „“Post-quantum cryptography is about proactively developing and building capabilities to secure critical information and systems from being compromised through the use of quantum computers,” said **Rob Joyce, Director of NSA Cybersecurity**.“
    - https://www.cisa.gov/news-events/news/cisa-nsa-and-nist-publish-new-resource-migrating-post-quantum-cryptography
- German approach
  - BSI TR-02102 Cryptographic Mechanisms
  - BSI, together with European partner authorities, has concretized the goal of completing the migration to quantum-safe mechanisms to protect against the “Store Now, Decrypt Later”-scenario for highly sensitive applications by the end of 2030 at the latest. 2026 starting date…
    - https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf
- NCSC, ETSI, and many more

How much time is left?



To estimate when the migration to quantum-safe cryptography is necessary, the following consideration by theoretical physicist M. Mosca from [Mos15] is very illustrative.

Let

- *x* be the number of years that the data to be protected must remain secured,
- *y* be the number of years needed to convert the corresponding system to quantum computer-resistant cryptography, and
- *z* be the number of years it will take for quantum computers to exist that threaten the cryptography currently in use.

Then, if x+y > z, you have a problem!

Figure: Illustration of "Mosca's Theorem"

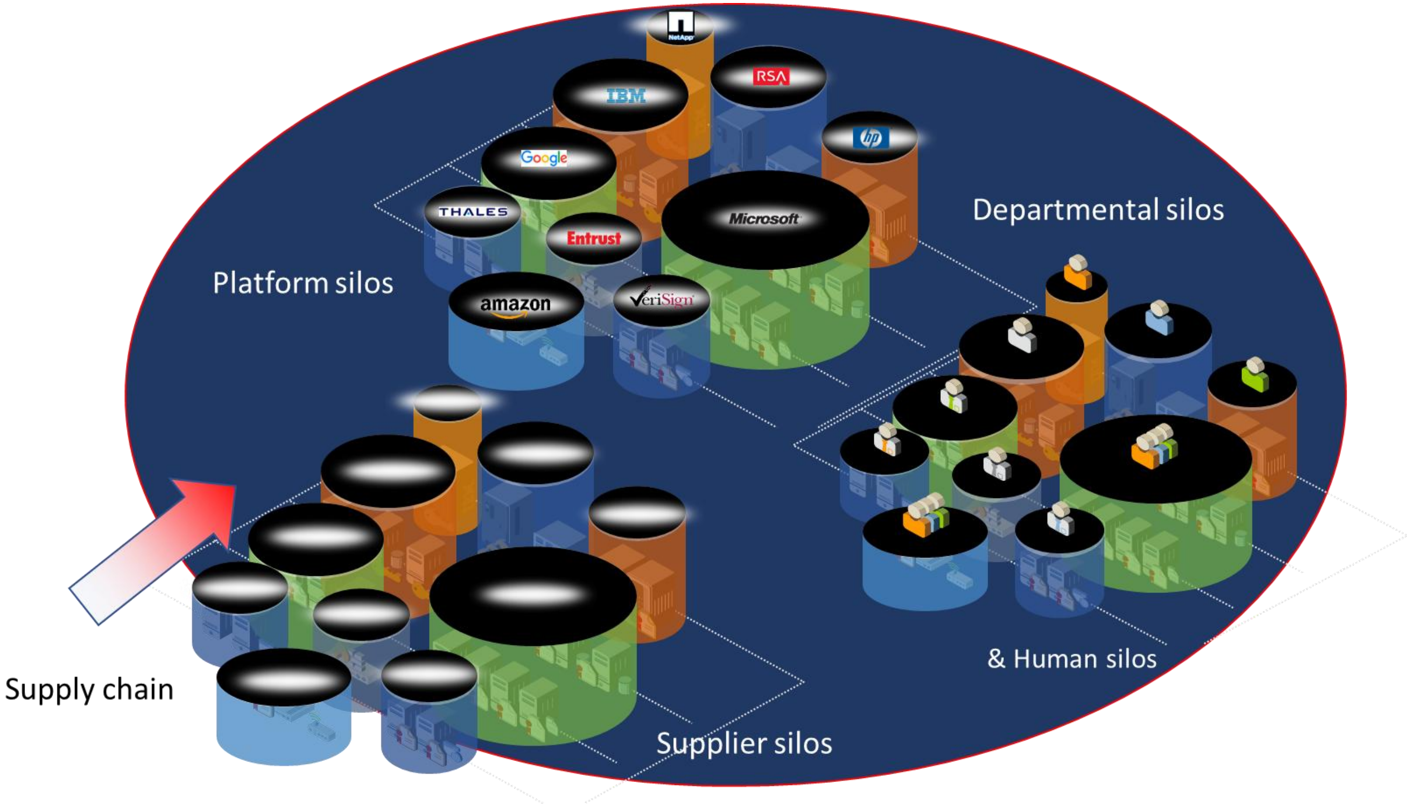
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf

Timelines in average

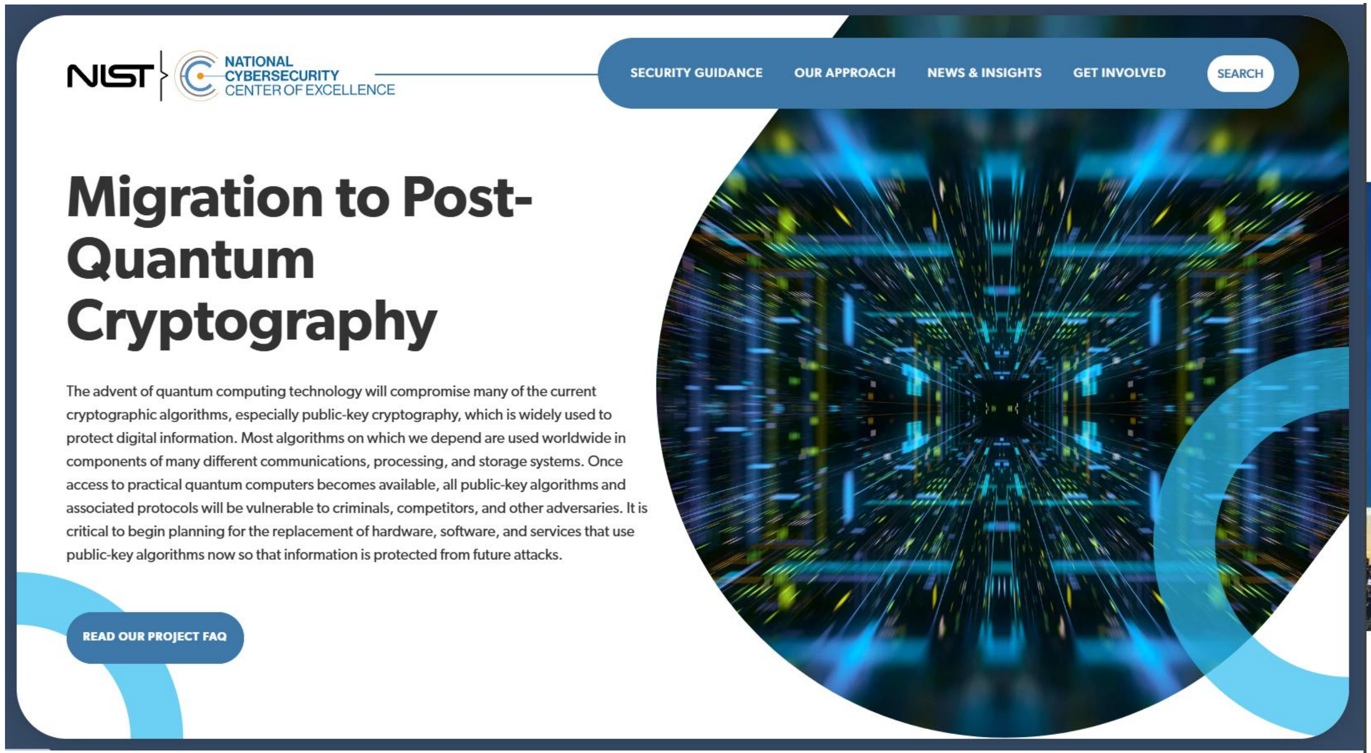
- 2026 – start preparations
    - Build teams, assign budget
    - Identify priorities /risks (e.g. cryptographic inventory, risk assessments)
    - Plan the migration
- 2030 – begin migration
    - Migrate, test, roll out
- 2035 – Quantum readyness
- Uncertainities: Attack to Lattice algorithms with Grover (Yes, not Shore)
    - Published first 2020 retracted due to a bug
        - Mid 2025 Publishing the bug was solved.
    - Argument for cryptographic agility (maybe redo all the work again) as acontinuous process

Data-Warehouse GmbH
Cybersecurity

Do you have a solution for your environment?



NCCoE & ACID … nope … ACDI- CADI

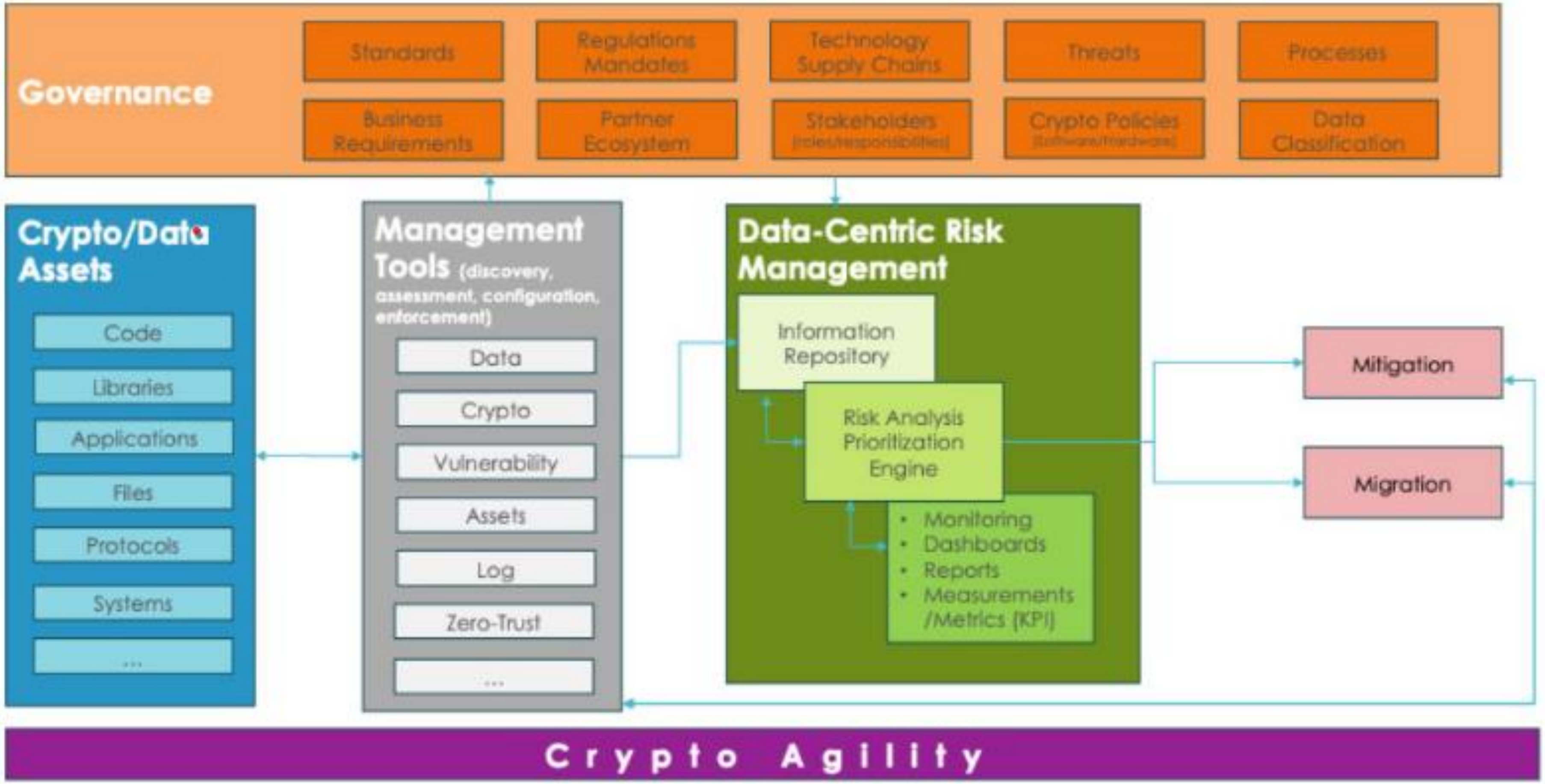


Migration to Post-Quantum Cryptography

The advent of quantum computing technology will compromise many of the current cryptographic algorithms, especially public-key cryptography, which is widely used to protect digital information. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to criminals, competitors, and other adversaries. It is critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

Strategy for Migrating to Automated Post-Quantum Cryptography Discovery and Inventory Tools

https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms h



Governance

Standards

Regulations Mandates

Technology Supply Chains

Threats

Processes

Business Requirements

Partner Ecosystem

Stakeholders (roles/responsibilities)

Crypto Policies (Software/Hardware)

Data Classification

Crypto/Data Assets

Code

Libraries

Applications

Files

Protocols

Systems

...

Management Tools (discovery, assessment, configuration, enforcement)

Data

Crypto

Vulnerability

Assets

Log

Zero-Trust

...

Data-Centric Risk Management

Information Repository

Risk Analysis Prioritization Engine

- Monitoring
- Dashboards
- Reports
- Measurements /Metrics (KPI)

Mitigation

Migration

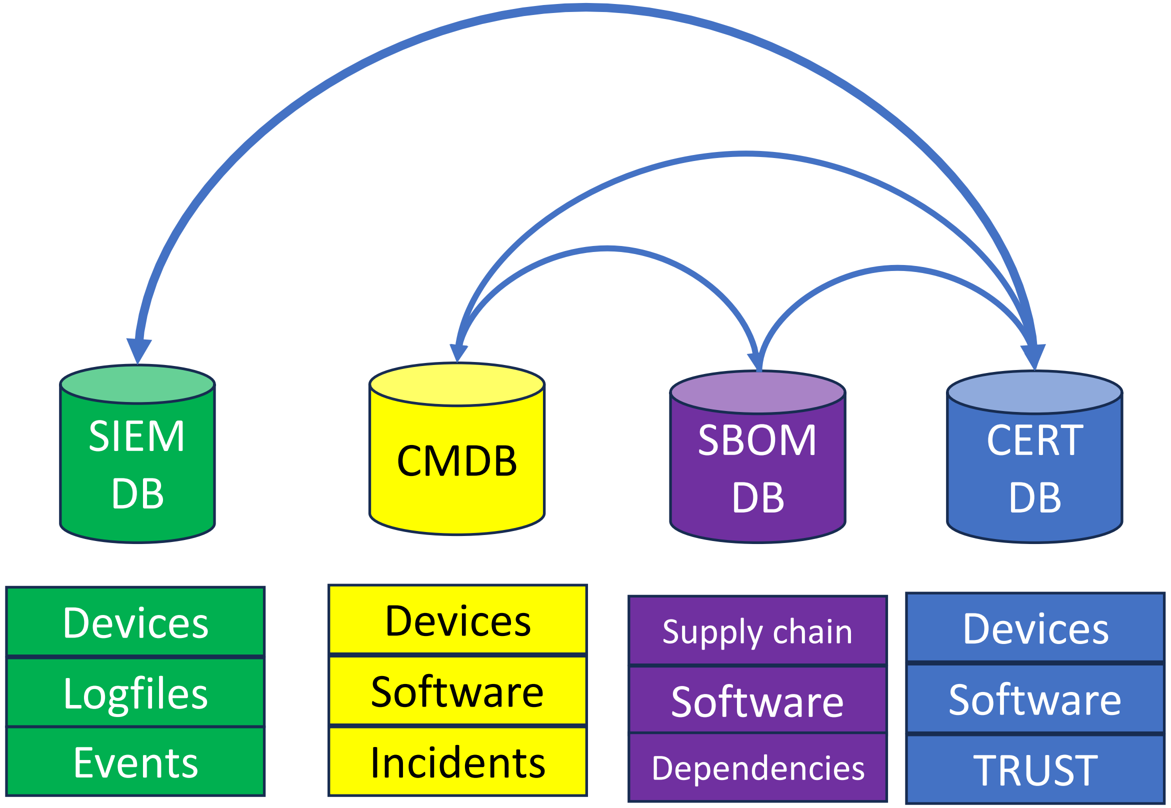
Crypto Agility

Let‘s start with the inventory

- Several different approaches to achieve the inventory
  - Using existing information systems and databases
  - Tracing the network traffic to find active cryptographic assets
  - Active scanning of the assets
  - Interfacing with existing cybersecurity agents to enrich the inventory

Approach one: Using existing information systems and databases

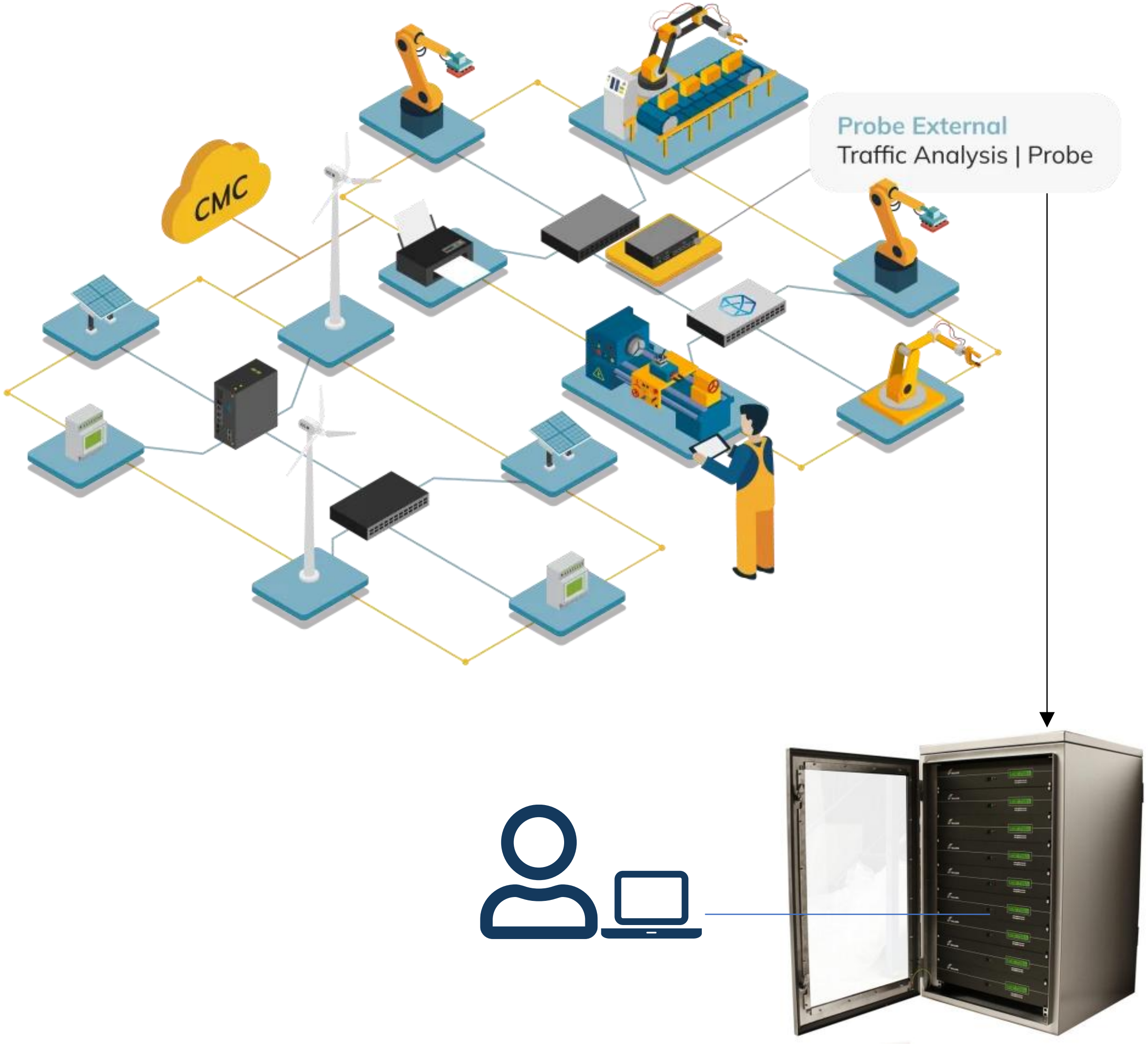
- Interfacing between the systems
- Extract existing cryptographic informations
- Pro:
  - No inpact to existing infrastructure (esp.complex one‘s)
- Con:
  - Only partial informations available due to quality of DB‘s
  - Interfacing topics



Approach two: Tracing the network traffic to find active cryptographic assets

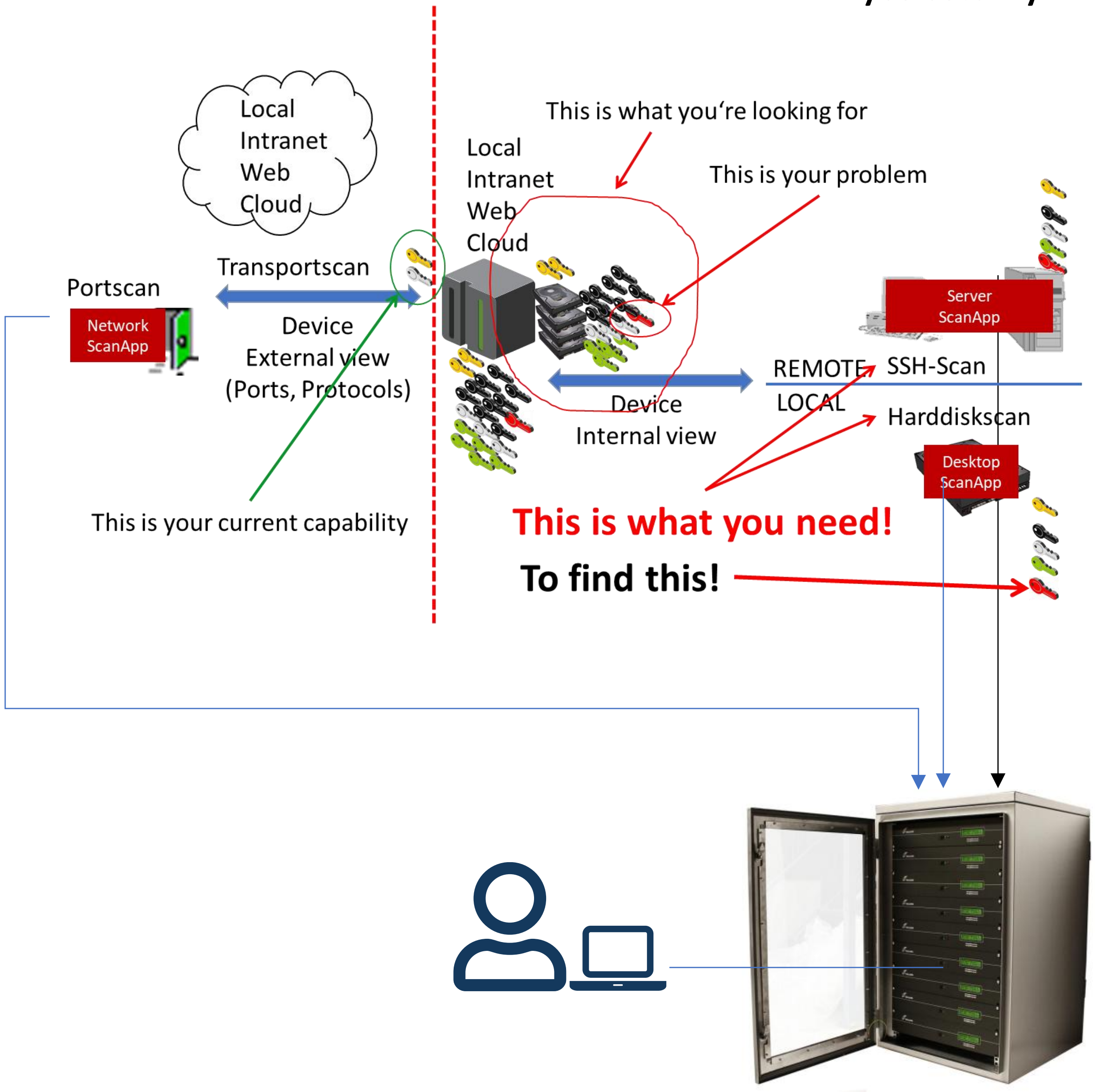
Data-Warehouse GmbH
Cybersecurity

- Sniffing the network with agents / probes / appliances
- Extract actively used cryptographic informations
- Pro:
  - Actively used crypto assets are detected
  - No third party tool needed
- Con:
  - Impact to infrastructure (Security)
  - External view to devices and coms (public keys). Additional effords for correct location and private key material needed



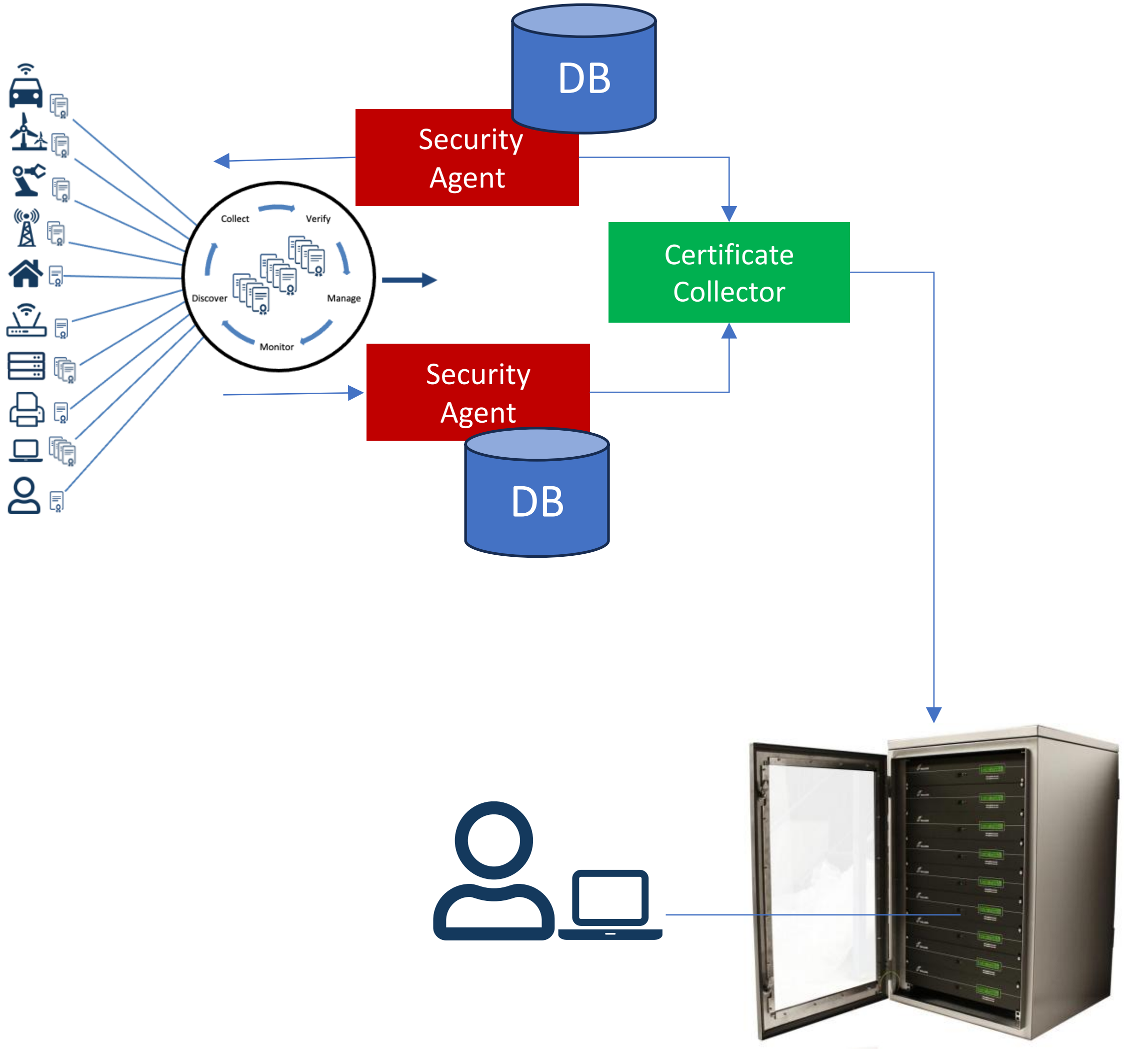
Approach three: Deep scanning cryptographic assets

- Combining network ports scanning and local scanning of all assets
- Extract all cryptographic informations (certificates, keys)
- Pro:
  - All used and stored crypto assets are detected
  - Permanent monitoring of cryptoassets
  - Deep informations to every assets
- Con:
  - Impact to infrastructure (Agents)
  - Data amount and time for implementation

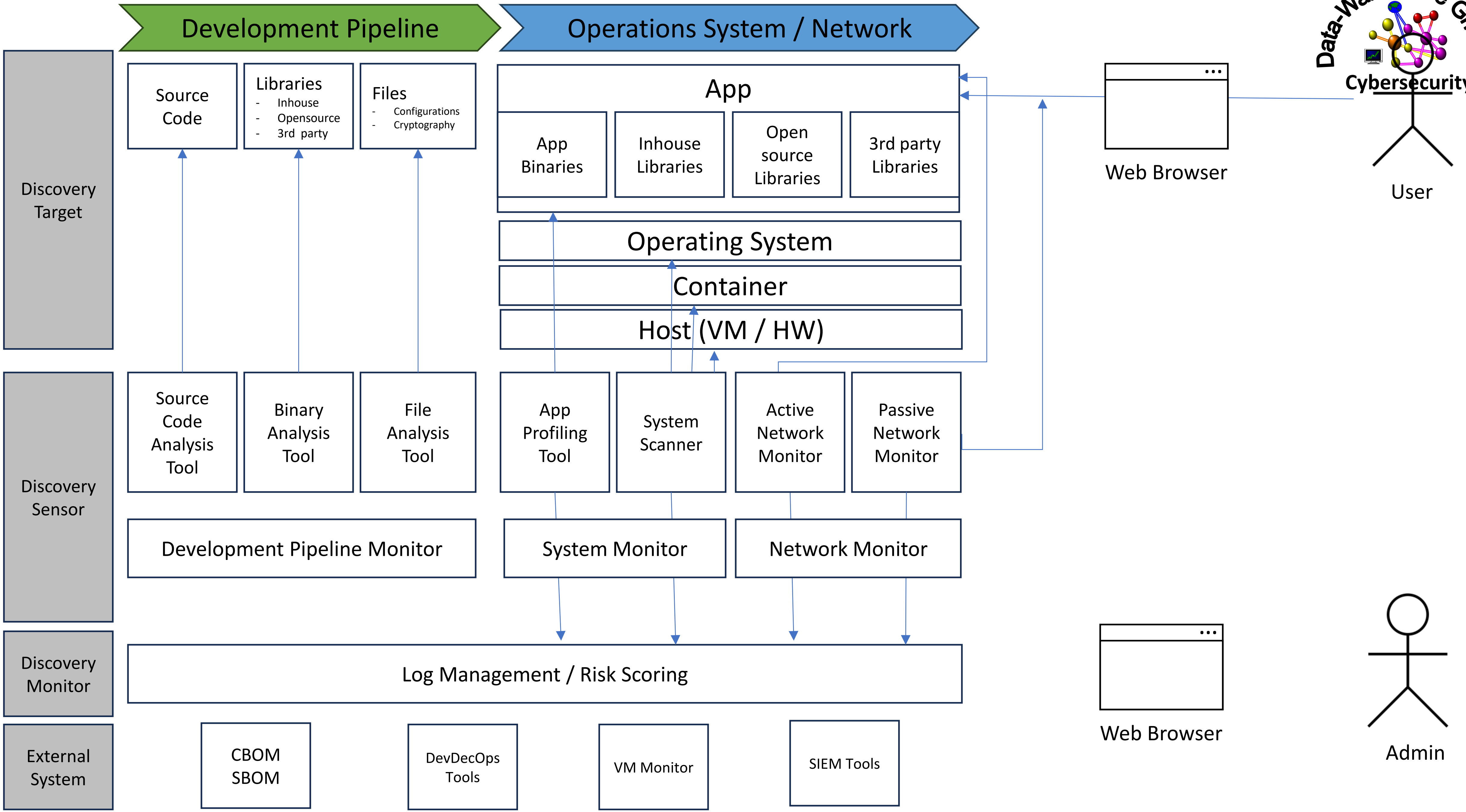


Approach four: Interfacing with existing cybersecurity agents to enrich the inventory

- Combining network ports scanning and local scanning of all assets
- Extract all cryptographic informations (certificates, keys)
- Pro:
  - All used and stored crypto assets are detected
  - Permanent monitoring of cryptoassets
  - Deep informations to every assets
- Con:
  - Impact to infrastructure (Agents)
  - Data amount and time for implementation



Data-Warehouse GmbH
Cybersecurity



Development Pipeline

Operations System / Network

Discovery Target

Source Code

Libraries
- Inhouse
- Opensource
- 3rd party

Files
- Configurations
- Cryptography

App

App Binaries

Inhouse Libraries

Open source Libraries

3rd party Libraries

Operating System

Container

Host (VM / HW)

Web Browser

User

Discovery Sensor

Source Code Analysis Tool

Binary Analysis Tool

File Analysis Tool

App Profiling Tool

System Scanner

Active Network Monitor

Passive Network Monitor

Development Pipeline Monitor

System Monitor

Network Monitor

Discovery Monitor

Log Management / Risk Scoring

External System

CBOM
SBOM

DevDecOps Tools

VM Monitor

SIEM Tools

Web Browser

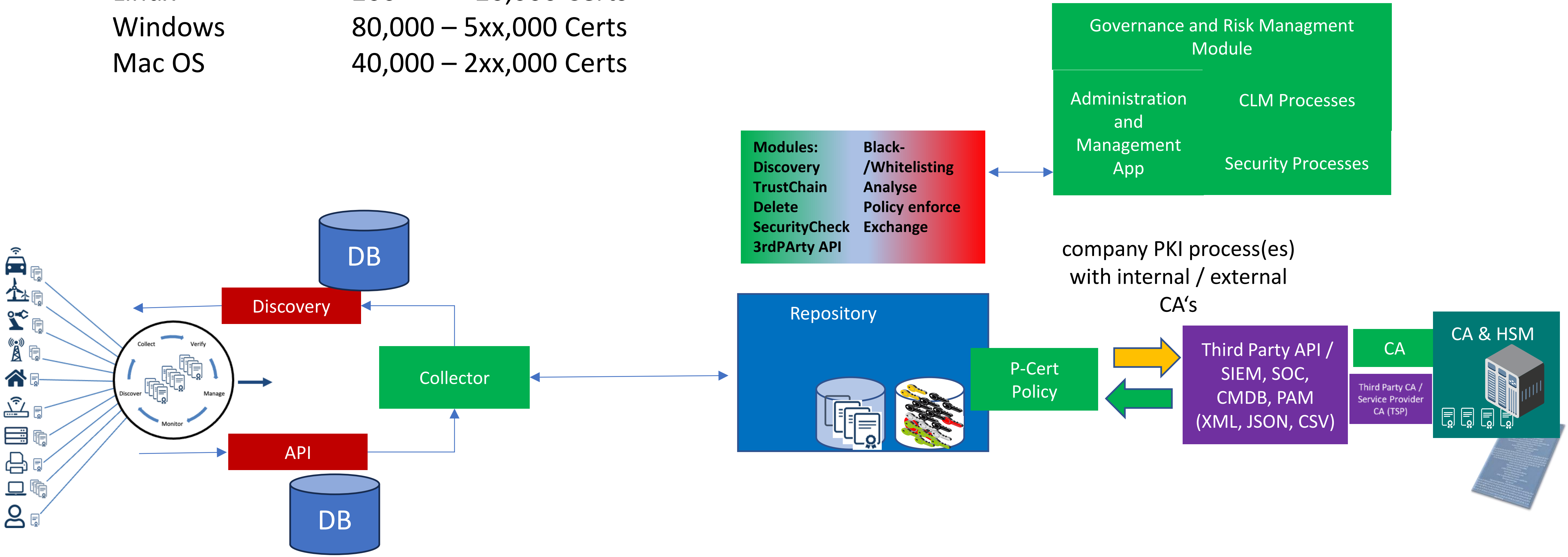
Admin

Practical samles & talking about numbers

Data-Warehouse GmbH Cybersecurity

Some numbers per device:

Linux	200 - 20,000 Certs
Windows	80,000 – 5xx,000 Certs
Mac OS	40,000 – 2xx,000 Certs



Governance and Risk Managment Module

Administration and Management App

CLM Processes

Security Processes

Modules: Discovery TrustChain Delete SecurityCheck 3rdPArty API

Black-/Whitelisting Analyse Policy enforce Exchange

company PKI process(es) with internal / external CA's

DB

Discovery

Collector

API

DB

Repository

P-Cert Policy

Third Party API / SIEM, SOC, CMDB, PAM (XML, JSON, CSV)

CA

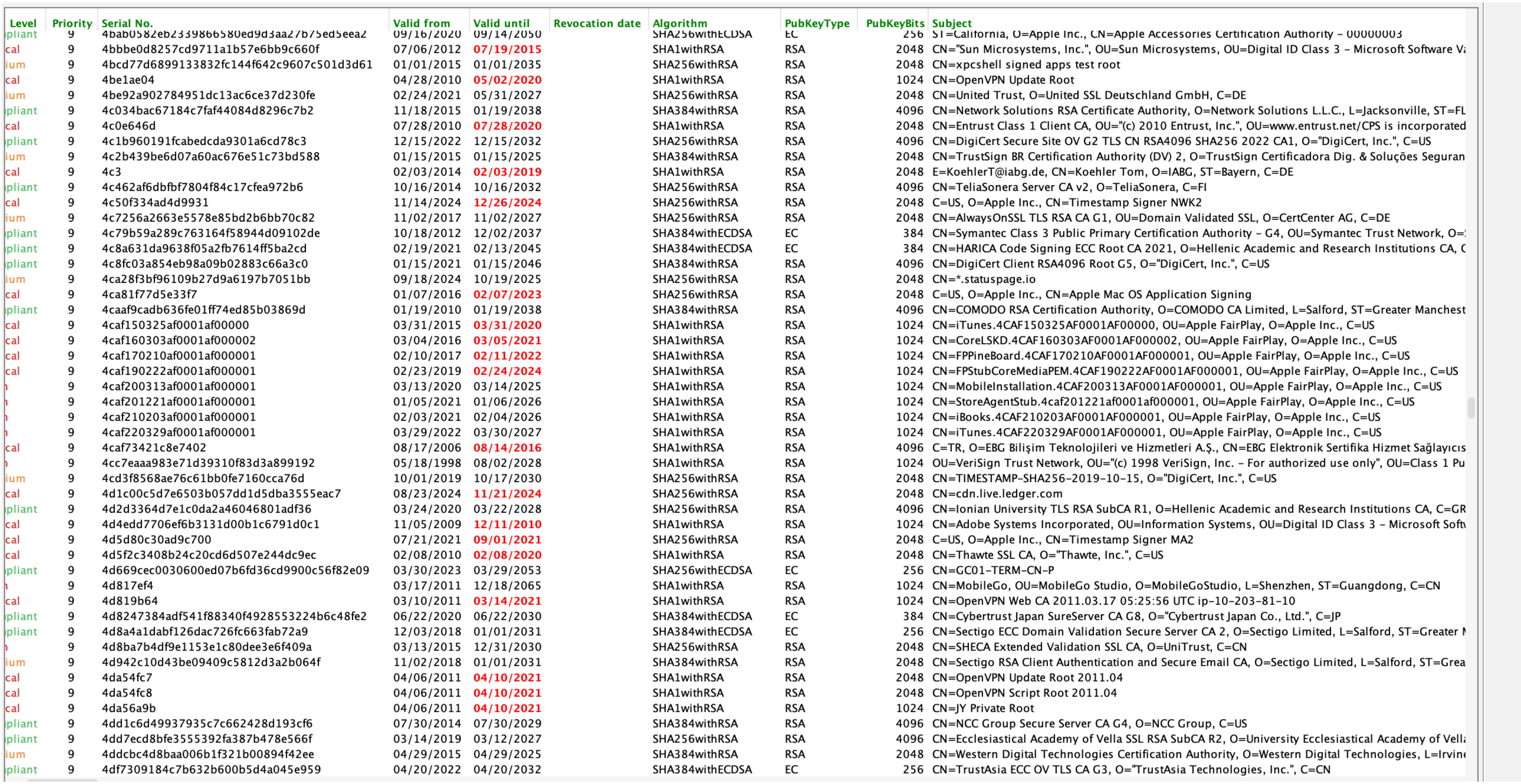
Third Party CA / Service Provider CA (TSP)

CA & HSM

Discovery and Visibility | Collection & Mitigation | Governance & Management

Cryptographic inventory example

Data-Warehouse GmbH
Cybersecurity

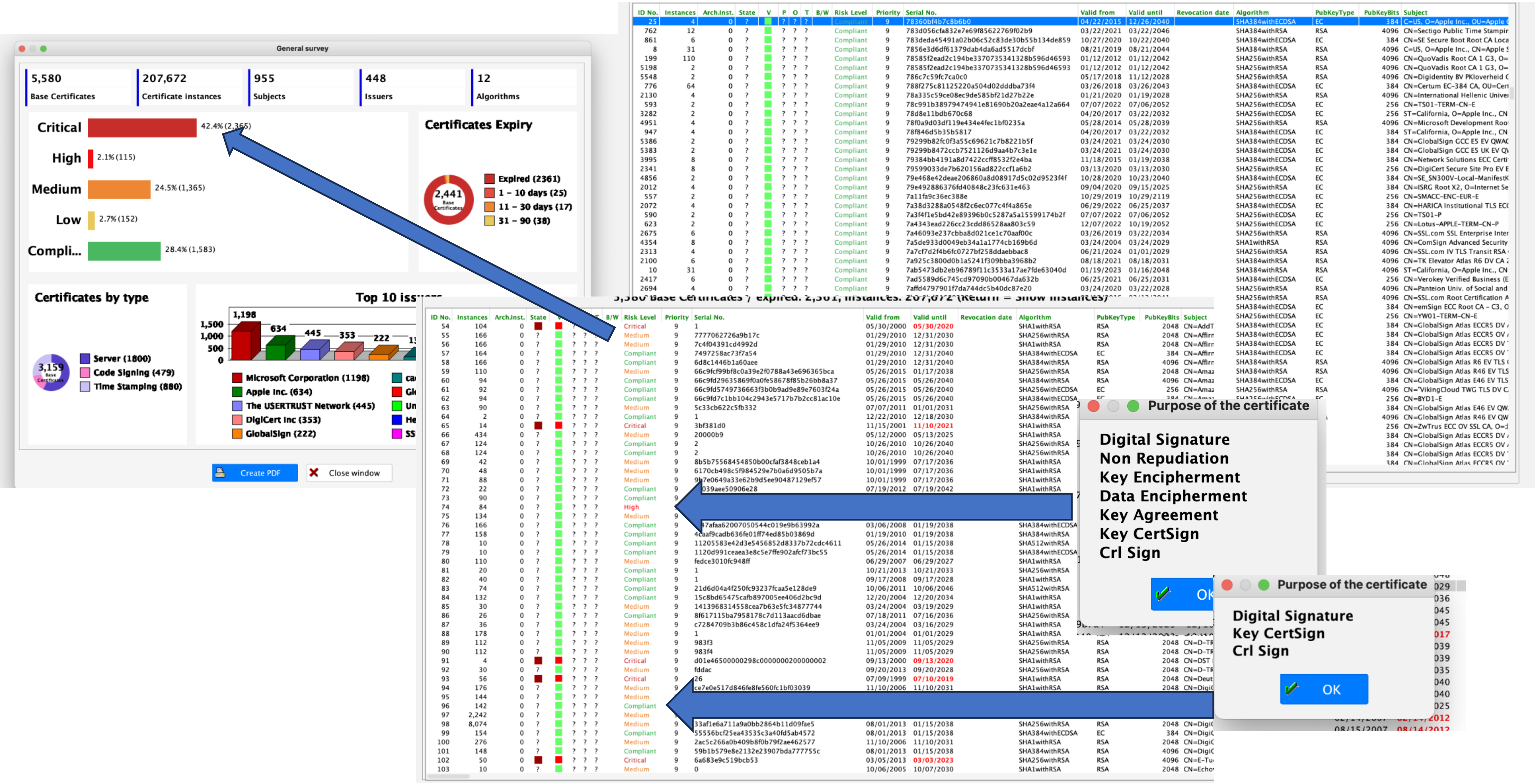


Level	Priority	Serial No.	Valid from	Valid until	Revocation date	Algorithm	PubKeyType	PubKeyBits	Subject
pliant	9	4bab0582eb2339866580ed9d3aa27b75ed5eea2	09/16/2020	09/14/2050		SHA256withECDSA	EC	256	ST=California, O=Apple Inc., CN=Apple Accessories Certification Authority – 00000003
cal	9	4bbbe0d8257cd9711a1b57e6bb9c660f	07/06/2012	07/19/2015		SHA1withRSA	RSA	2048	CN="Sun Microsystems, Inc.", OU=Sun Microsystems, OU=Digital ID Class 3 – Microsoft Software Va
ium	9	4bcd77d6899133832fc144f642c9607c501d3d61	01/01/2015	01/01/2035		SHA256withRSA	RSA	2048	CN=xpcshell signed apps test root
cal	9	4be1ae04	04/28/2010	05/02/2020		SHA1withRSA	RSA	1024	CN=OpenVPN Update Root
ium	9	4be92a902784951dc13ac6ce37d230fe	02/24/2021	05/31/2027		SHA256withRSA	RSA	2048	CN=United Trust, O=United SSL Deutschland GmbH, C=DE
pliant	9	4c034bac67184c7faf44084d8296c7b2	11/18/2015	01/19/2038		SHA384withRSA	RSA	4096	CN=Network Solutions RSA Certificate Authority, O=Network Solutions L.L.C., L=Jacksonville, ST=FL
cal	9	4c0e646d	07/28/2010	07/28/2020		SHA1withRSA	RSA	2048	CN=Entrust Class 1 Client CA, OU="(c) 2010 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated
pliant	9	4c1b960191fcabedcda9301a6cd78c3	12/15/2022	12/15/2032		SHA256withRSA	RSA	4096	CN=DigiCert Secure Site OV G2 TLS CN RSA4096 SHA256 2022 CA1, O="DigiCert, Inc.", C=US
ium	9	4c2b439be6d07a60ac676e51c73bd588	01/15/2015	01/15/2025		SHA384withRSA	RSA	2048	CN=TrustSign BR Certification Authority (DV) 2, O=TrustSign Certificadora Dig. & Soluções Seguran
cal	9	4c3	02/03/2014	02/03/2019		SHA1withRSA	RSA	2048	E=KoehlerT@iabg.de, CN=Koehler Tom, O=IABG, ST=Bayern, C=DE
pliant	9	4c462af6dbfbf7804f84c17cfea972b6	10/16/2014	10/16/2032		SHA256withRSA	RSA	4096	CN=TeliaSonera Server CA v2, O=TeliaSonera, C=FI
cal	9	4c50f334ad4d9931	11/14/2024	12/26/2024		SHA256withRSA	RSA	2048	C=US, O=Apple Inc., CN=Timestamp Signer NWK2
ium	9	4c7256a2663e5578e85bd2b6bb70c82	11/02/2017	11/02/2027		SHA256withRSA	RSA	2048	CN=AlwaysOnSSL TLS RSA CA G1, OU=Domain Validated SSL, O=CertCenter AG, C=DE
pliant	9	4c79b59a289c763164f58944d09102de	10/18/2012	12/02/2037		SHA384withECDSA	EC	384	CN=Symantec Class 3 Public Primary Certification Authority – G4, OU=Symantec Trust Network, O=:
pliant	9	4c8a631da9638f05a2fb7614ff5ba2cd	02/19/2021	02/13/2045		SHA384withECDSA	EC	384	CN=HARICA Code Signing ECC Root CA 2021, O=Hellenic Academic and Research Institutions CA, C
pliant	9	4c8fc03a854eb98a09b02883c66a3c0	01/15/2021	01/15/2046		SHA384withRSA	RSA	4096	CN=DigiCert Client RSA4096 Root G5, O="DigiCert, Inc.", C=US
ium	9	4ca28f3bf96109b27d9a6197b7051bb	09/18/2024	10/19/2025		SHA256withRSA	RSA	2048	CN=*.statuspage.io
cal	9	4ca81f77d5e33f7	01/07/2016	02/07/2023		SHA256withRSA	RSA	2048	C=US, O=Apple Inc., CN=Apple Mac OS Application Signing
pliant	9	4caaf9cadb636fe01ff74ed85b03869d	01/19/2010	01/19/2038		SHA384withRSA	RSA	4096	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchest
cal	9	4caf150325af0001af00000	03/31/2015	03/31/2020		SHA1withRSA	RSA	1024	CN=iTunes.4CAF150325AF0001AF00000, OU=Apple FairPlay, O=Apple Inc., C=US
cal	9	4caf160303af0001af000002	03/04/2016	03/05/2021		SHA1withRSA	RSA	1024	CN=CoreLSKD.4CAF160303AF0001AF000002, OU=Apple FairPlay, O=Apple Inc., C=US
cal	9	4caf170210af0001af000001	02/10/2017	02/11/2022		SHA1withRSA	RSA	1024	CN=FPPineBoard.4CAF170210AF0001AF000001, OU=Apple FairPlay, O=Apple Inc., C=US
cal	9	4caf190222af0001af000001	02/23/2019	02/24/2024		SHA1withRSA	RSA	1024	CN=FPStubCoreMediaPEM.4CAF190222AF0001AF000001, OU=Apple FairPlay, O=Apple Inc., C=US
h	9	4caf200313af0001af000001	03/13/2020	03/14/2025		SHA1withRSA	RSA	1024	CN=MobileInstallation.4CAF200313AF0001AF000001, OU=Apple FairPlay, O=Apple Inc., C=US
h	9	4caf201221af0001af000001	01/05/2021	01/06/2026		SHA1withRSA	RSA	1024	CN=StoreAgentStub.4caf201221af0001af000001, OU=Apple FairPlay, O=Apple Inc., C=US
h	9	4caf210203af0001af000001	02/03/2021	02/04/2026		SHA1withRSA	RSA	1024	CN=iBooks.4CAF210203AF0001AF000001, OU=Apple FairPlay, O=Apple Inc., C=US
h	9	4caf220329af0001af000001	03/29/2022	03/30/2027		SHA1withRSA	RSA	1024	CN=iTunes.4CAF220329AF0001AF000001, OU=Apple FairPlay, O=Apple Inc., C=US
cal	9	4caf73421c8e7402	08/17/2006	08/14/2016		SHA1withRSA	RSA	4096	C=TR, O=EBG Bilişim Teknolojileri ve Hizmetleri A.Ş., CN=EBG Elektronik Sertifika Hizmet Sağlayıcıs
h	9	4cc7eaaa983e71d39310f83d3a899192	05/18/1998	08/02/2028		SHA1withRSA	RSA	1024	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. – For authorized use only", OU=Class 1 Pu
ium	9	4cd3f8568ae76c61bb0fe7160cca76d	10/01/2019	10/17/2030		SHA256withRSA	RSA	2048	CN=TIMESTAMP-SHA256-2019-10-15, O="DigiCert, Inc.", C=US
cal	9	4d1c00c5d7e6503b057dd1d5dba3555eac7	08/23/2024	11/21/2024		SHA256withRSA	RSA	2048	CN=cdn.live.ledger.com
pliant	9	4d2d3364d7e1c0da2a46046801adf36	03/24/2020	03/22/2028		SHA256withRSA	RSA	4096	CN=Ionian University TLS RSA SubCA R1, O=Hellenic Academic and Research Institutions CA, C=GR
cal	9	4d4edd7706ef6b3131d00b1c6791d0c1	11/05/2009	12/11/2010		SHA1withRSA	RSA	1024	CN=Adobe Systems Incorporated, OU=Information Systems, OU=Digital ID Class 3 – Microsoft Softv
cal	9	4d5d80c30ad9c700	07/21/2021	09/01/2021		SHA256withRSA	RSA	2048	C=US, O=Apple Inc., CN=Timestamp Signer MA2
cal	9	4d5f2c3408b24c20cd6d507e244dc9ec	02/08/2010	02/08/2020		SHA1withRSA	RSA	2048	CN=Thawte SSL CA, O="Thawte, Inc.", C=US
pliant	9	4d669cec0030600ed07b6fd36cd9900c56f82e09	03/30/2023	03/29/2053		SHA256withECDSA	EC	256	CN=GC01-TERM-CN-P
h	9	4d817ef4	03/17/2011	12/18/2065		SHA1withRSA	RSA	1024	CN=MobileGo, OU=MobileGo Studio, O=MobileGoStudio, L=Shenzhen, ST=Guangdong, C=CN
cal	9	4d819b64	03/10/2011	03/14/2021		SHA1withRSA	RSA	1024	CN=OpenVPN Web CA 2011.03.17 05:25:56 UTC ip-10-203-81-10
pliant	9	4d8247384adf541f88340f4928553224b6c48fe2	06/22/2020	06/22/2030		SHA384withECDSA	EC	384	CN=Cybertrust Japan SureServer CA G8, O="Cybertrust Japan Co., Ltd.", C=JP
pliant	9	4d8a4a1dabf126dac726fc663fab72a9	12/03/2018	01/01/2031		SHA384withECDSA	EC	256	CN=Sectigo ECC Domain Validation Secure Server CA 2, O=Sectigo Limited, L=Salford, ST=Greater M
h	9	4d8ba7b4df9e1153e1c80dee3e6f409a	03/13/2015	12/31/2030		SHA256withRSA	RSA	2048	CN=SHECA Extended Validation SSL CA, O=UniTrust, C=CN
ium	9	4d942c10d43be09409c5812d3a2b064f	11/02/2018	01/01/2031		SHA384withRSA	RSA	2048	CN=Sectigo RSA Client Authentication and Secure Email CA, O=Sectigo Limited, L=Salford, ST=Grea
cal	9	4da54fc7	04/06/2011	04/10/2021		SHA1withRSA	RSA	2048	CN=OpenVPN Update Root 2011.04
cal	9	4da54fc8	04/06/2011	04/10/2021		SHA1withRSA	RSA	2048	CN=OpenVPN Script Root 2011.04
cal	9	4da56a9b	04/06/2011	04/10/2021		SHA1withRSA	RSA	1024	CN=JY Private Root
pliant	9	4dd1c6d49937935c7c662428d193cf6	07/30/2014	07/30/2029		SHA384withRSA	RSA	4096	CN=NCC Group Secure Server CA G4, O=NCC Group, C=US
pliant	9	4dd7ecd8bfe3555392fa387b478e566f	03/14/2019	03/12/2027		SHA256withRSA	RSA	4096	CN=Ecclesiastical Academy of Vella SSL RSA SubCA R2, O=University Ecclesiastical Academy of Vella
ium	9	4ddcbc4d8baa006b1f321b00894f42ee	04/29/2015	04/29/2025		SHA384withRSA	RSA	2048	CN=Western Digital Technologies Certification Authority, O=Western Digital Technologies, L=Irvine
pliant	9	4df7309184c7b632b600b5d4a045e959	04/20/2022	04/20/2032		SHA384withECDSA	EC	256	CN=TrustAsia ECC OV TLS CA G3, O="TrustAsia Technologies, Inc.", C=CN

Like numbers? Mac Osx Highscore: currently 256.000, MS Windows 10: 369.000 Certs&Keys on one device

Risk Assessment option example

Data-Warehouse GmbH
Cybersecurity



5,580 Base Certificates

207,672 Certificate instances

955 Subjects

448 Issuers

12 Algorithms

Critical	42.4% (2,365)
High	2.1% (115)
Medium	24.5% (1,365)
Low	2.7% (152)
Compli...	28.4% (1,583)

Certificates Expiry

- Expired (2361)
- 1 – 10 days (25)
- 11 – 30 days (17)
- 31 – 90 (38)

Certificates by type

- Server (1800)
- Code Signing (479)
- Time Stamping (880)

Top 10 issuers

- Microsoft Corporation (1198)
- Apple Inc. (634)
- The USERTRUST Network (445)
- DigiCert Inc (353)
- GlobalSign (222)
- ca
- Gl
- Un
- He
- SS

ID No.	Instances	Arch.Inst.	State	V	P	O	T	B/W	Risk Level	Priority	Serial No.	Valid from	Valid until	Revocation date	Algorithm	PubKeyType	PubKeyBits	Subject
25	4	0	?	🟩	?	?	?		Compliant	9	78360bf4b7c8b6b0	04/22/2015	12/26/2040		SHA384withECDSA	EC	384	C=US, O=Apple Inc., OU=Apple
762	12	0	?	🟩	?	?	?		Compliant	9	783d056cfa832e7e69f85622769f02b9	03/22/2021	03/22/2046		SHA384withRSA	RSA	4096	CN=Sectigo Public Time Stampir
861	6	0	?	🟩	?	?	?		Compliant	9	783deda45491a02b06c52c83de30b55b134de859	10/27/2020	10/22/2040		SHA384withECDSA	EC	384	CN=SE Secure Boot Root CA Loca
8	31	0	?	🟩	?	?	?		Compliant	9	7856e3d6df61379dab4da6ad5517dcbf	08/21/2019	08/21/2044		SHA384withRSA	RSA	4096	C=US, O=Apple Inc., CN=Apple
199	110	0	?	🟩	?	?	?		Compliant	9	78585f2ead2c194be3370735341328b596d46593	01/12/2012	01/12/2042		SHA256withRSA	RSA	4096	CN=QuoVadis Root CA 1 G3, O=
5198	2	0	?	🟩	?	?	?		Compliant	9	78585f2ead2c194be3370735341328b596d46593	01/12/2012	01/12/2042		SHA256withRSA	RSA	4096	CN=QuoVadis Root CA 1 G3, O=
5548	2	0	?	🟩	?	?	?		Compliant	9	786c7c59fc7ca0c0	05/17/2018	11/12/2028		SHA256withRSA	RSA	4096	CN=Digidentity BV PKIoverheid
776	64	0	?	🟩	?	?	?		Compliant	9	788f275c81125220a504d02dddba73f4	03/26/2018	03/26/2043		SHA384withECDSA	EC	384	CN=Certum EC-384 CA, OU=Cert
2130	4	0	?	🟩	?	?	?		Compliant	9	78a335c59ce08ec9de585bf21d27b22e	01/21/2020	01/19/2028		SHA256withRSA	RSA	4096	CN=International Hellenic Univer
593	2	0	?	🟩	?	?	?		Compliant	9	78c991b38979474941e81690b20a2eae4a12a664	07/07/2022	07/06/2052		SHA256withECDSA	EC	256	CN=TS01-TERM-CN-E
3282	2	0	?	🟩	?	?	?		Compliant	9	78d8e11bdb670c68	04/20/2017	03/22/2032		SHA256withECDSA	EC	256	ST=California, O=Apple Inc., CN
4951	4	0	?	🟩	?	?	?		Compliant	9	78f0a9d03df119e434e4fec1bf0235a	05/28/2014	05/28/2039		SHA256withRSA	RSA	4096	CN=Microsoft Development Roo
947	4	0	?	🟩	?	?	?		Compliant	9	78f846d5b35b5817	04/20/2017	03/22/2032		SHA384withECDSA	EC	384	ST=California, O=Apple Inc., CN
5386	2	0	?	🟩	?	?	?		Compliant	9	79299b82fc0f3a55c69621c7b8221b5f	03/24/2021	03/24/2030		SHA384withECDSA	EC	384	CN=GlobalSign GCC E5 EV QWAC
5383	2	0	?	🟩	?	?	?		Compliant	9	79299b8472ccb7521126d9aa4b7c3e1e	03/24/2021	03/24/2030		SHA384withECDSA	EC	384	CN=GlobalSign GCC E5 UK EV Q
3995	8	0	?	🟩	?	?	?		Compliant	9	79384bb4191a8d7422ccff8532f2e4ba	11/18/2015	01/19/2038		SHA384withECDSA	EC	384	CN=Network Solutions ECC Certi
2341	8	0	?	🟩	?	?	?		Compliant	9	79599033de7b620156ad822ccf1a6b2	03/13/2020	03/13/2030		SHA256withRSA	EC	256	CN=DigiCert Secure Site Pro EV E
4856	2	0	?	🟩	?	?	?		Compliant	9	79e468e42deae206860a8d08917d5c02d9523f4f	10/28/2020	10/23/2040		SHA384withECDSA	EC	384	CN=SE_SN300V-Local-ManifestK
2012	4	0	?	🟩	?	?	?		Compliant	9	79e492886376fd40848c23fc631e463	09/04/2020	09/15/2025		SHA256withRSA	EC	384	CN=ISRG Root X2, O=Internet Se
557	2	0	?	🟩	?	?	?		Compliant	9	7a11fa9c36ec388e	10/29/2019	10/29/2119		SHA256withECDSA	EC	256	CN=SMACC-ENC-EUR-E
2072	4	0	?	🟩	?	?	?		Compliant	9	7a38d3288a0548f2c6ec077c4f4a865e	06/29/2022	06/25/2037		SHA384withECDSA	EC	384	CN=HARICA Institutional TLS ECC
590	2	0	?	🟩	?	?	?		Compliant	9	7a3f4f1e5bd42e89396b0c5287a5a15599174b2f	07/07/2022	07/06/2052		SHA256withECDSA	EC	256	CN=TS01-P
623	2	0	?	🟩	?	?	?		Compliant	9	7a4343ead226cc23cdd86528aa803c59	12/07/2022	10/19/2052		SHA256withECDSA	EC	256	CN=Lotus-APPLE-TERM-CN-P
2675	6	0	?	🟩	?	?	?		Compliant	9	7a46093e237cbba8d021ce1c70aaf00c	03/26/2019	03/22/2034		SHA256withRSA	RSA	4096	CN=SSL.com SSL Enterprise Inter
4354	8	0	?	🟩	?	?	?		Compliant	9	7a5de933d0049eb34a1a1774cb169b6d	03/24/2004	03/24/2029		SHA1withRSA	RSA	4096	CN=ComSign Advanced Security
2313	4	0	?	🟩	?	?	?		Compliant	9	7a7cf7d2f4b6fc0727bf258ddaebbac8	06/21/2024	01/01/2029		SHA256withRSA	RSA	4096	CN=SSL.com IV TLS Transit RSA
2100	6	0	?	🟩	?	?	?		Compliant	9	7a925c3800d0b1a5241f309bba3968b2	08/18/2021	08/18/2031		SHA384withRSA	RSA	4096	CN=TK Elevator Atlas R6 DV CA
10	31	0	?	🟩	?	?	?		Compliant	9	7ab5473db2eb96789f11c3533a17ae7fde63040d	01/19/2023	01/16/2048		SHA384withRSA	RSA	4096	ST=California, O=Apple Inc., CN
2417	6	0	?	🟩	?	?	?		Compliant	9	7ad5589d6c745cd97090b00467da632b	06/25/2021	06/25/2031		SHA384withECDSA	EC	256	CN=Verokey Verified Business (E
2694	4	0	?	🟩	?	?	?		Compliant	9	7affd4797901f7da744dc5b40dc87e20	03/24/2020	03/22/2028		SHA256withRSA	RSA	4096	CN=Panteion Univ. of Social and
															SHA256withRSA	RSA	4096	CN=SSL.com Root Certification A
															SHA384withECDSA	EC	384	CN=emSign ECC Root CA – C3, O
															SHA256withECDSA	EC	256	CN=YW01-TERM-CN-E
															SHA384withECDSA	EC	384	CN=GlobalSign Atlas ECCR5 DV
															SHA384withECDSA	EC	384	CN=GlobalSign Atlas ECCR5 OV
															SHA384withECDSA	EC	384	CN=GlobalSign Atlas ECCR5 DV
															SHA384withECDSA	EC	384	CN=GlobalSign Atlas ECCR5 OV
															SHA384withRSA	RSA	4096	CN=GlobalSign Atlas R6 EV TLS
															SHA384withRSA	RSA	4096	CN=GlobalSign Atlas R46 EV TLS
															SHA384withECDSA	EC	384	CN=GlobalSign Atlas E46 EV TLS
															SHA256withRSA	RSA	4096	CN='VikingCloud TWG TLS DV C
																	256	CN=BYD1-E
																	384	CN=GlobalSign Atlas E46 EV QW
																	4096	CN=GlobalSign Atlas R46 EV QW
																	256	CN=ZwTrus ECC OV SSL CA, O=
																	384	CN=GlobalSign Atlas ECCR5 DV
																	384	CN=GlobalSign Atlas ECCR5 OV
																	384	CN=GlobalSign Atlas ECCR5 DV
																	384	CN=GlobalSign Atlas ECCR5 OV

5,580 Base Certificates / expired: 2,361, instances: 207,672 (Return = Show instances)

ID No.	Instances	Arch.Inst.	State	V	P	O	T	B/W	Risk Level	Priority	Serial No.	Valid from	Valid until	Revocation date	Algorithm	PubKeyType	PubKeyBits	Subject
54	104	0	■	🟥	?				Critical	9	1	05/30/2000	05/30/2020		SHA1withRSA	RSA	2048	CN=AddT
55	166	0	?	🟩	?	?			Medium	9	7777062726a9b17c	01/29/2010	12/31/2030		SHA256withRSA	RSA	2048	CN=Affir
56	166	0	?	🟩	?	?	?		Medium	9	7c4f04391cd4992d	01/29/2010	12/31/2030		SHA1withRSA	RSA	2048	CN=Affir
57	164	0	?	🟩	?	?	?		Compliant	9	7497258ac73f7a54	01/29/2010	12/31/2040		SHA384withECDSA	EC	384	CN=Affir
58	166	0	?	🟩	?	?	?		Compliant	9	6d8c1446b1a60aee	01/29/2010	12/31/2040		SHA384withRSA	RSA	4096	CN=Affir
59	110	0	?	🟩	?	?	?		Medium	9	66c9fcf99bf8c0a39e2f0788a43e696365bca	05/26/2015	01/17/2038		SHA256withRSA	RSA	2048	CN=Amaz
60	94	0	?	🟩	?	?	?		Compliant	9	66c9fd29635869f0a0fe58678f85b26bb8a37	05/26/2015	05/26/2040		SHA384withRSA	RSA	4096	CN=Amaz
61	92	0	?	🟩	?	?	?		Compliant	9	66c9fd5749736663f3b0b9ad9e89e7603f24a	05/26/2015	05/26/2040		SHA256withECDSA	EC	256	CN=Amaz
62	94	0	?	🟩	?	?	?		Compliant	9	66c9fd7c1bb104c2943e5717b7b2cc81ac10e	05/26/2015	05/26/2040		SHA384withECDSA	EC	384	CN=Ama
63	90	0	?	🟩	?	?	?		Medium	9	5c33cb622c5fb332	07/07/2011	01/01/2031		SHA256withRSA			
64	2	0	?	🟩	?	?	?		Compliant	9	1	12/22/2010	12/18/2030		SHA384withRSA			
65	14	0	■	🟥	?	?	?		Critical	9	3bf381d0	11/15/2001	11/10/2021		SHA1withRSA			
66	434	0	?	🟩	?	?	?		Medium	9	20000b9	05/12/2000	05/13/2025		SHA1withRSA			
67	124	0	?	🟩	?	?	?		Compliant	9	2	10/26/2010	10/26/2040		SHA256withRSA			
68	124	0	?	🟩	?	?	?		Compliant	9	2	10/26/2010	10/26/2040		SHA256withRSA			
69	42	0	?	🟩	?	?	?		Medium	9	8b5b75568454850b00cfaf3848ceb1a4	10/01/1999	07/17/2036		SHA1withRSA			
70	48	0	?	🟩	?	?	?		Medium	9	6170cb498c5f984529e7b0a6d9505b7a	10/01/1999	07/17/2036		SHA1withRSA			
71	88	0	?	🟩	?	?	?		Medium	9	9b7e0649a33e62b9d5ee90487129ef57	10/01/1999	07/17/2036		SHA1withRSA			
72	22	0	?	🟩	?	?	?		Compliant	9	039aee50906e28	07/19/2012	07/19/2042		SHA1withRSA			
73	90	0	?	🟩	?	?	?		Compliant	9								
74	84	0	?	🟩	?	?	?		High									
75	134	0	?	🟩	?	?	?		Medium	9								
76	166	0	?	🟩	?	?	?		Compliant	9	47afaa62007050544c019e9b63992a	03/06/2008	01/19/2038		SHA384withECDSA			
77	158	0	?	🟩	?	?	?		Compliant	9	4caaf9cadb636fe01ff74ed85b03869d	01/19/2010	01/19/2038		SHA384withRSA			
78	10	0	?	🟩	?	?	?		Compliant	9	11205583e42d3e5456852d8337b72cdc4611	05/26/2014	01/15/2038		SHA512withRSA			
79	10	0	?	🟩	?	?	?		Compliant	9	1120d991ceaea3e8c5e7ffe902afcf73bc55	05/26/2014	01/15/2038		SHA384withECDSA			
80	110	0	?	🟩	?	?	?		Medium	9	fedce3010fc948ff	06/29/2007	06/29/2027		SHA1withRSA			
81	20	0	?	🟩	?	?	?		Compliant	9	1	10/21/2013	10/21/2033		SHA256withRSA			
82	40	0	?	🟩	?	?	?		Compliant	9	1	09/17/2008	09/17/2028		SHA1withRSA			
83	74	0	?	🟩	?	?	?		Compliant	9	21d6d04a4f250fc93237fcaa5e128de9	10/06/2011	10/06/2046		SHA512withRSA			
84	132	0	?	🟩	?	?	?		Compliant	9	15c8bd65475cafb897005ee406d2bc9d	12/20/2004	12/20/2034		SHA1withRSA			
85	30	0	?	🟩	?	?	?		Medium	9	1413968314558cea7b63e5fc34877744	03/24/2004	03/19/2029		SHA1withRSA			
86	26	0	?	🟩	?	?	?		Compliant	9	8f617115ba7958178c7d113aacd6dbae	07/18/2011	07/16/2036		SHA256withRSA			
87	36	0	?	🟩	?	?	?		Medium	9	c7284709b3b86c458c1dfa24f5364ee9	03/24/2004	03/16/2029		SHA1withRSA			
88	178	0	?	🟩	?	?	?		Medium	9	1	01/01/2004	01/01/2029		SHA1withRSA			
89	112	0	?	🟩	?	?	?		Medium	9	983f3	11/05/2009	11/05/2029		SHA256withRSA	RSA	2048	CN=D-TR
90	112	0	?	🟩	?	?	?		Medium	9	983f4	11/05/2009	11/05/2029		SHA256withRSA	RSA	2048	CN=D-TR
91	4	0	■	🟥	?	?	?		Critical	9	d01e46500000298c000000200000002	09/13/2000	09/13/2020		SHA1withRSA	RSA	2048	CN=DST
92	30	0	?	🟩	?	?	?		Medium	9	fddac	09/20/2013	09/20/2028		SHA256withRSA	RSA	2048	CN=D-TR
93	56	0	■	🟥	?	?	?		Critical	9	26	07/09/1999	07/10/2019		SHA1withRSA	RSA	2048	CN=Deut
94	176	0	?	🟩	?	?	?		Medium	9	ce7e0e517d846fe8fe560fc1bf03039	11/10/2006	11/10/2031		SHA1withRSA	RSA	2048	CN=Digi
95	144	0	?	🟩	?	?	?		Medium									
96	142	0	?	🟩	?	?	?		Compliant									
97	2,242	0	?	🟩	?	?	?		Medium									
98	8,074	0	?	🟩	?	?	?		Medium	9	33af1e6a711a9a0bb2864b11d09fae5	08/01/2013	01/15/2038		SHA256withRSA	RSA	2048	CN=Digi
99	154	0	?	🟩	?	?	?		Compliant	9	55556bcf25ea43535c3a40fd5ab4572	08/01/2013	01/15/2038		SHA384withECDSA	EC	384	CN=Digi
100	276	0	?	🟩	?	?	?		Medium	9	2ac5c266a0b409b8f0b79f2ae462577	11/10/2006	11/10/2031		SHA1withRSA	RSA	2048	CN=Digi
101	148	0	?	🟩	?	?	?		Compliant	9	59b1b579e8e2132e23907bda777755c	08/01/2013	01/15/2038		SHA384withRSA	RSA	4096	CN=Digi
102	50	0	■	🟥	?	?	?		Critical	9	6a683e9c519bcb53	03/05/2013	03/03/2023		SHA256withRSA	RSA	4096	CN=E-Tu
103	10	0	?	🟩	?	?	?		Medium	9	0	10/06/2005	10/07/2030		SHA1withRSA	RSA	2048	CN=Echo

Purpose of the certificate

Digital Signature
Non Repudiation
Key Encipherment
Data Encipherment
Key Agreement
Key CertSign
Crl Sign

Purpose of the certificate

Digital Signature
Key CertSign
Crl Sign

Need for permanent process or onetime?

- Cryptographic inventory – CBOM++
  - Building a Cryptographic Bill of Material and consolidate it in enterprise context
- Software supply chain inventory – SBOM++
  - Building a Software Bill of Material and consolidate it in enterprise context
- Crypto agility
  - Changing from one cryptographic provider (CA) to another with maximum automation. Identify weaknesses and needs for exchanging cryptography
- Risk identification and monitoring
  - Identifying risk components or suppliers in the enterprise context
- Post Quantum Migration, Quantum Security
  - Identify Risks, setting priorities, select algorithmic, perform development, change cryptography, verify status, perform operation, maintain product, implement new technologies
- Investigate cryptographic security
  - Eg. Keystore security, key / cryptographic handling

Full Stop.

Data-Warehouse GmbH
Ottobrunn/Germany
https://datawh.info