

Post-Quantum

Cryptography Conference

## Practical Insights from Following NIST SP 1800-38B

In this session, Dr. Alexander Löw from Data-Warehouse will share real-world experiences from the National Cybersecurity Center of Excellence (NCCoE) regarding the implementation of NIST SP 1800-38B. Alexander will delve into the practical application of public key application discovery tools within the context of transitioning to PQC. Participants will gain insights into the step-by-step process outlined in SP 1800-38B, including identifying public key cryptographic algorithms in use, assessing their vulnerability to quantum attacks, developing a migration strategy, and implementing new PQC algorithms. By walking through the challenges encountered, attendees gain insights into what to expect during their transition, and learn about the role and benefits of Cryptographic Agility, Cryptographic Inventory, Cryptographic Bill of Material (CBOM), Software Bill of Material (SBOM), and Cryptographic Governance, providing comprehensive insights based on real-world experiences from following the National Cybersecurity Center of Excellence (NCCoE).



**Alexander Löw**  
CEO at Data-Warehouse



KEYFACTOR



January 15 and 16, 2025 - Austin, TX (US) | Online

PKI Consortium Inc. is registered as a 501(c)(6) non-profit entity ("business league") under Utah law (10462204-0140) | [pkic.org](https://pkic.org)



**PKI**  
Consortium

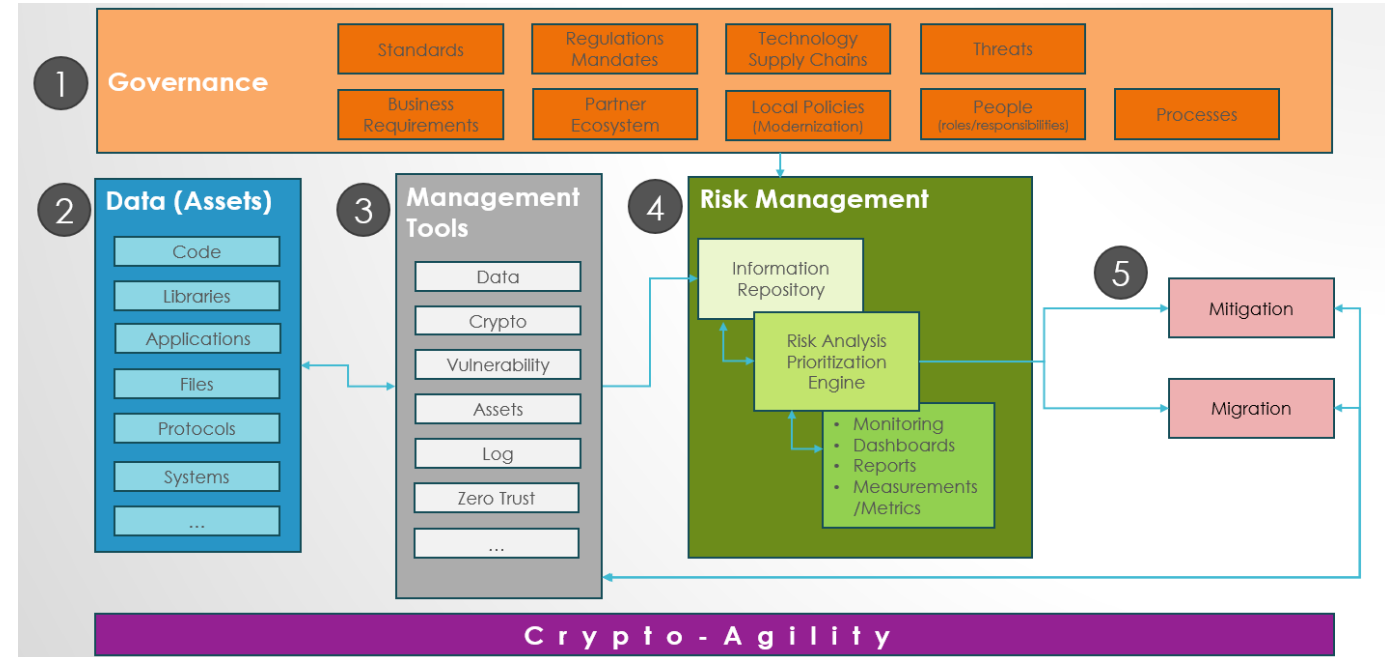
# Practical Insights from Following NIST SP 1800-38B

Alexander Loew

# Theoretical aspects

## Action Blocks 1-5

- 1 understanding the enterprise
- 2 collect data
- 3 manage the environment
- 4 perform risk management
- 5 perform the migration



# Takeaways and learnings from the WG

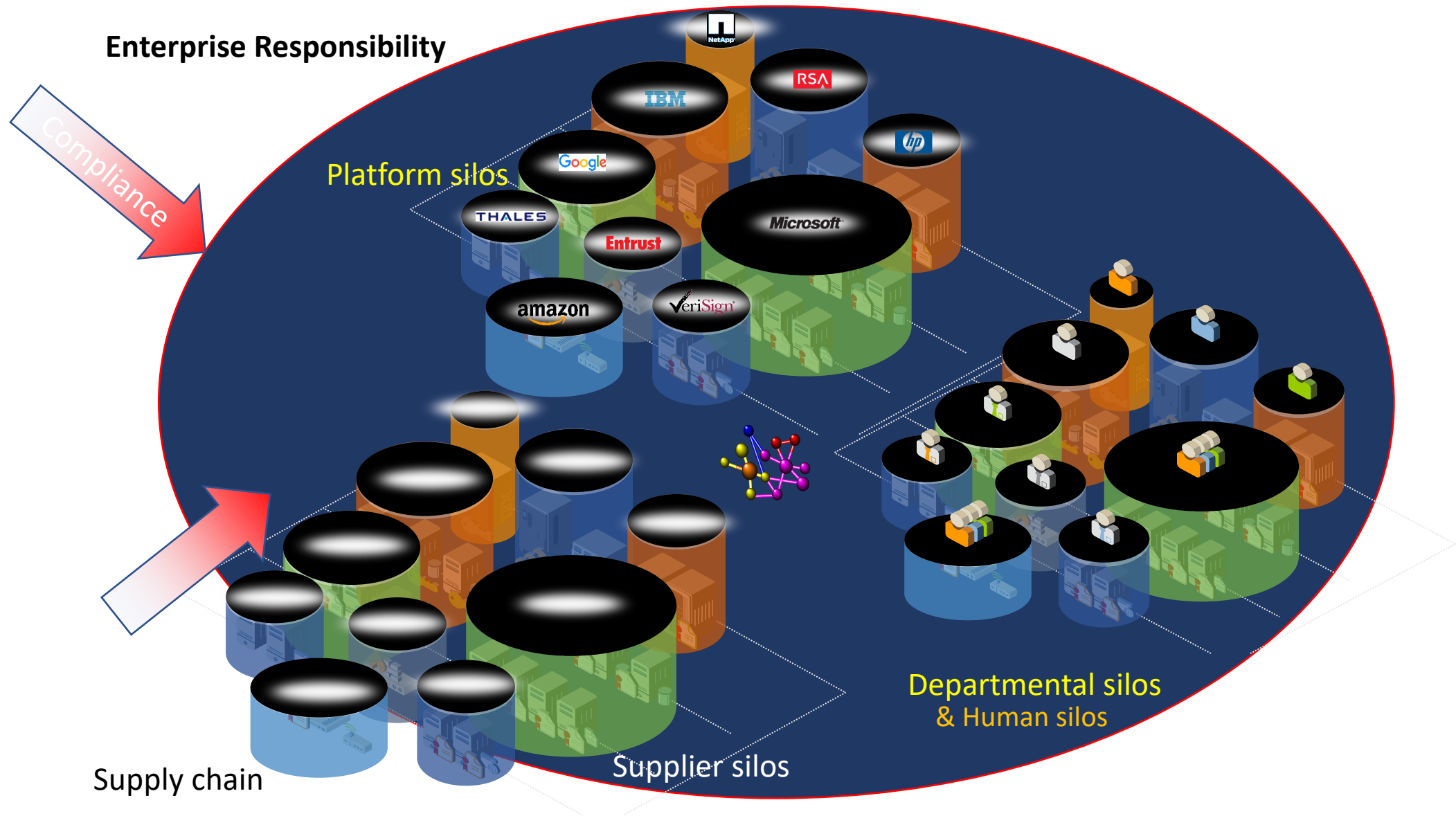
- Working on a standard is plenty of formal work
  - Many participants with different approaches / goals / motivations
  - Harmonization needs formal processes which are handled in Working Groups and Subgroups
- It is essential to generalize
  - Put away the product glasses and judging and be open to other ideas
  - Especially for techies a challenge ;-)
  - NIST must provide tech neutral guidelines
- If you like to participate plan enough resources to contribute
  - Even listening and learning from existing solutions and discussions bring new insights and ideas.

# Give aways about stepping into PQM

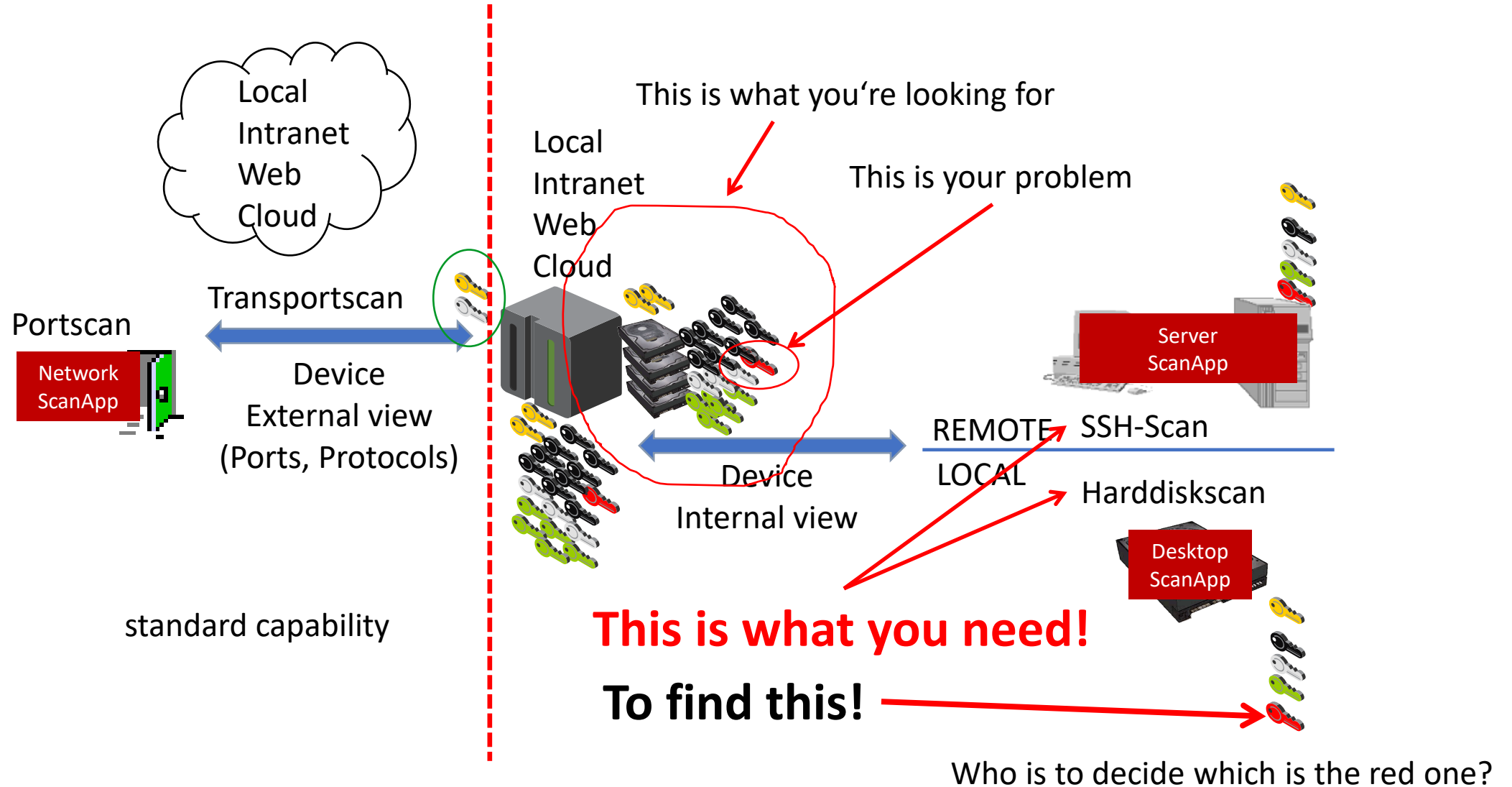


- Visibility
  - know your infrastructure
- Strategy
  - know your business traps, compliance and frameworks
- Legality
  - operate in a legal status and be able to proof it
- Interoperability
  - be able to interface with as many as possible stakeholders
- Flexibility
  - be able to adapt to any business and technological change
- Exchangeability
  - be able to transfer the current solution and data to another platform
- Automation
  - reduce manual and human interaction to a maximum within compliance

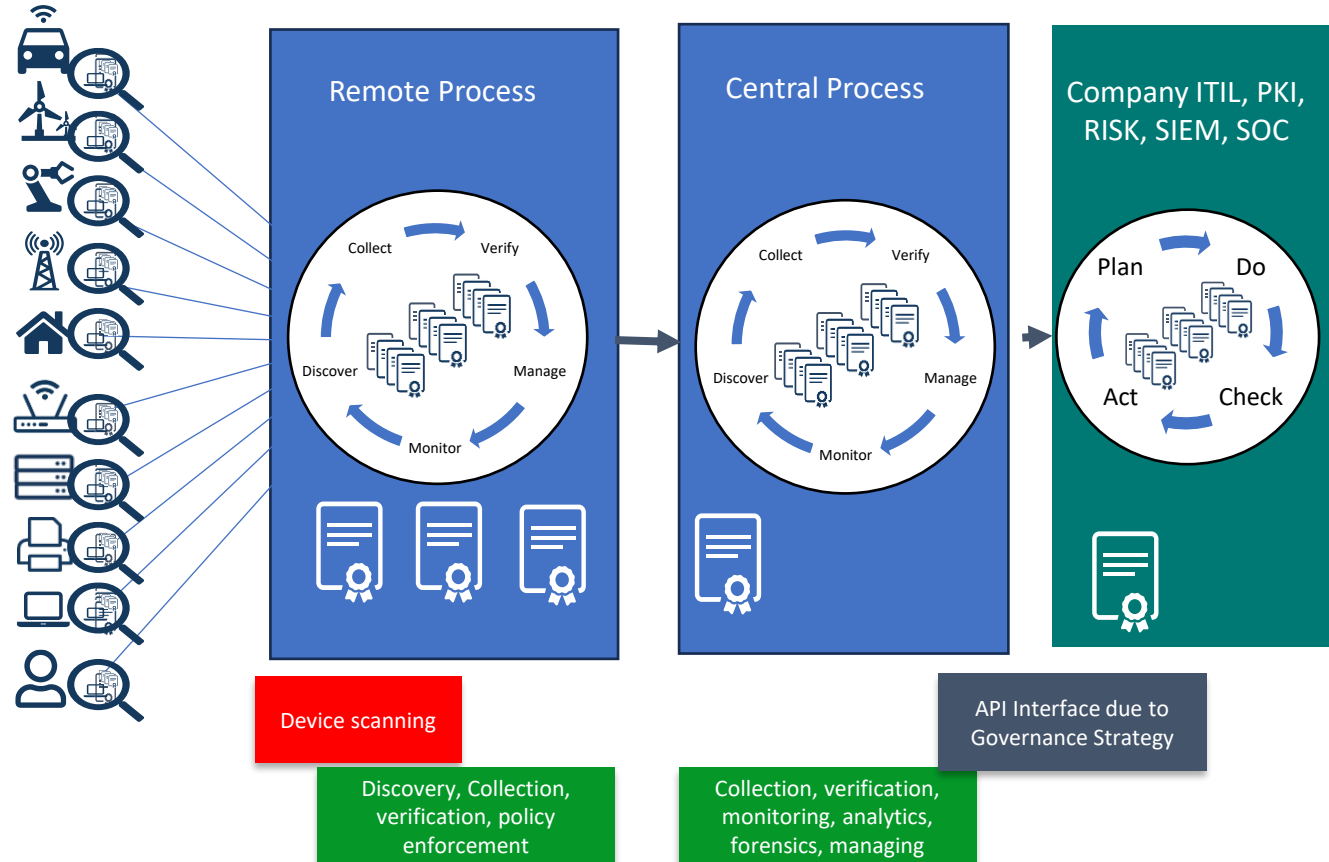
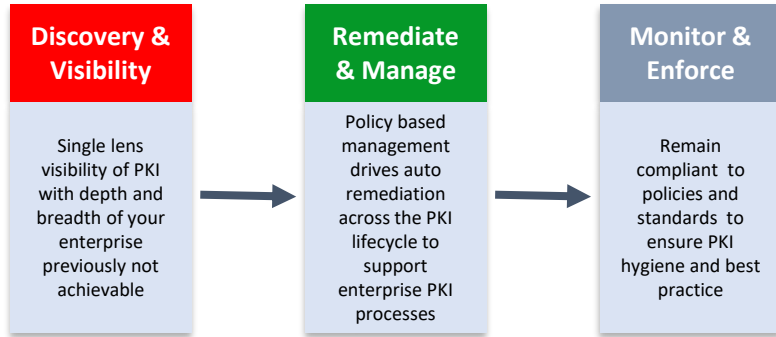
My understanding of the Challenge in trust silos and cryptography to be handled: why visibility?



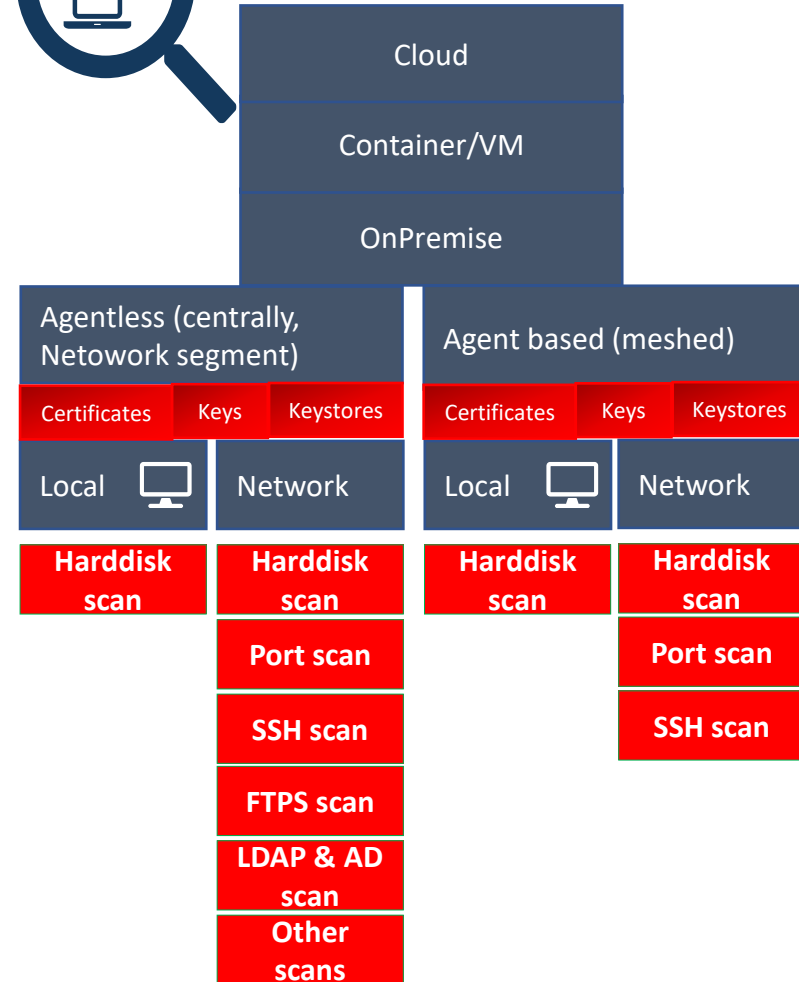
# Visibility challenge: Cryptographic discovery (one IT driven-Device)



# Cryptographic-Lifecycle-Management



# Discovery engines unveils the unknown unknowns to complete your infrastructure understanding





# Cryptographic inventory example



Level	Priority	Serial No.	Valid from	Valid until	Revocation date	Algorithm	PubKeyType	PubKeyBits	Subject
pliant	9	4bab0582eb2339866580ed9d3aa27b75ed5eeaz	09/16/2020	09/14/2050		SHA256withECDSA	EC	256	SI=California, O=Apple Inc., CN=Apple Accessories Certification Authority - 00000003
cal	9	4bbbe0d8257cd9711a1b57e6bb9c660f	07/06/2012	<b>07/19/2015</b>		SHA1withRSA	RSA	2048	CN="Sun Microsystems, Inc.", OU=Sun Microsystems, OU=Digital ID Class 3 - Microsoft Software V
ium	9	4bcd77d6899133832fc144f642c9607c501d3d61	01/01/2015	01/01/2035		SHA256withRSA	RSA	2048	CN=xpcshell signed apps test root
cal	9	4be1ae04	04/28/2010	<b>05/02/2020</b>		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	4c034bac67184c7faf440848d296c7b2	11/18/2015	01/19/2038		SHA256withRSA	RSA	4096	CN=Network Solutions RSA Certificate Authority, O=Network Solutions L.L.C., L=Jacksonville, ST=FL
cal	9	4c0e646d	07/28/2010	<b>07/28/2020</b>		SHA1withRSA	RSA	2048	CN=Entrust Class 1 Client CA, OU="(c) 2010 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated
pliant	9	4c1b960191fcbacedca9301a6cd78c3	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	<b>02/03/2019</b>		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	<b>12/26/2024</b>		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	4ca81f7745e33f7	01/07/2016	<b>02/07/2023</b>		SHA256withRSA	RSA	2048	C=US, O=Apple Inc., CN=Apple Mac OS Application Signing
pliant	9	4caaf9caddb636fe01ff74ed85b03869d	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	<b>03/31/2020</b>		SHA1withRSA	RSA	1024	CN=iTunes.4CAF150325AF0001AF000000, OU=Apple FairPlay, O=Apple Inc., C=US
cal	9	4caf160303af0001af000002	03/04/2016	<b>03/05/2021</b>		SHA1withRSA	RSA	1024	CN=CoreLSKD.4CAF160303AF0001AF000002, OU=Apple FairPlay, O=Apple Inc., C=US
cal	9	4caf170210af0001af000001	02/10/2017	<b>02/11/2022</b>		SHA1withRSA	RSA	1024	CN=FPineBoard.4CAF170210AF0001AF000001, OU=Apple FairPlay, O=Apple Inc., C=US
cal	9	4caf190222af0001af000001	02/23/2019	<b>02/24/2024</b>		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	<b>08/14/2016</b>		SHA1withRSA	RSA	4096	C=TR, O=EBG Bilişim Teknolojileri ve Hizmetleri A.Ş., CN=EBG Elektronik Sertifika Hizmet Sağlayıcısı
h	9	4cc7eaa983e71d39310f83d3a899192	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	<b>11/21/2024</b>		SHA256withRSA	RSA	2048	CN=cdn.live.ledger.com
pliant	9	4d2d3364d7e1c0da2a46046801ad3f6	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	<b>12/11/2010</b>		SHA1withRSA	RSA	1024	CN=Adobe Systems Incorporated, OU=Information Systems, OU=Digital ID Class 3 - Microsoft Soft
cal	9	4d5d80c30ad9c700	07/21/2021	<b>09/01/2021</b>		SHA256withRSA	RSA	2048	C=US, O=Apple Inc., CN=Timestamp Signer MA2
cal	9	4d5f2c3408b24c20cd6d507e244dc9ec	02/08/2010	<b>02/08/2020</b>		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	<b>03/14/2021</b>		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	06/22/2020		SHA384withECDSA	EC	384	CN=Cybertrust Japan SureServer CA G8, O="Cybertrust Japan Co., Ltd.", C=JP
pliant	9	4d84a1dabf126dac726fc663fab72a9	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 I
h	9	4d8ba7b4df9e1153e1c80dee3e6f409a	03/13/2015	12/31/2030		SHA256withRSA	RSA	2048	CN=SHCA 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	<b>04/10/2021</b>		SHA1withRSA	RSA	2048	CN=OpenVPN Update Root 2011.04
cal	9	4da54fc8	04/06/2011	<b>04/10/2021</b>		SHA1withRSA	RSA	2048	CN=OpenVPN Script Root 2011.04
cal	9	4da56a9b	04/06/2011	<b>04/10/2021</b>		SHA1withRSA	RSA	1024	CN=JY Private Root
pliant	9	4dd1c6d49937935c7c662428d193cf6	07/30/2014	07/30/2014		SHA384withRSA	RSA	4096	CN=NCC Group Secure Server CA G4, O=NCC Group, C=US
pliant	9	4dd7ecd8bfe355392fa387b478e566f	03/14/2019	03/12/2027		SHA256withRSA	RSA	4096	CN=Ecclesiastical Academy of Vella SSL RSA SubCA R2, O=University Ecclesiastical Academy of Velli
ium	9	4ddcbb4d8baa006b1f321b00894f42ee	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



General survey

5,580 Base Certificates | 207,672 Certificate instances | 955 Subjects | 448 Issuers | 12 Algorithms

**Certificates Expiry**

- Critical: 42.4% (2,365)
- High: 2.1% (115)
- Medium: 24.5% (1,365)
- Low: 2.7% (152)
- Compliant: 28.4% (1,583)

**2,441 Base Certificates**

- 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)

Create PDF | Close window

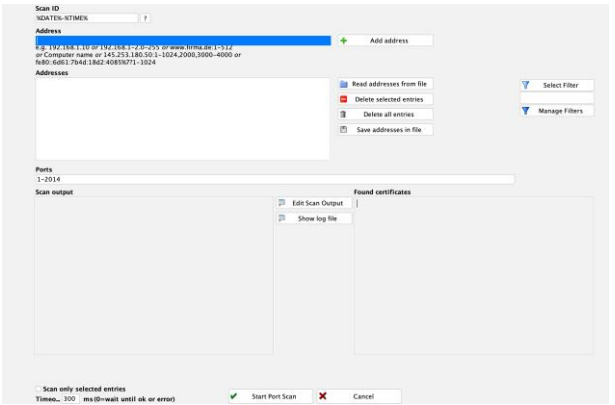
ID No.	Instances	Arch.Inst.	State	V	P	O	T	R/W	Risk Level	Priority	Serial No.	Valid from	Valid until	Revocation date	Algorithm	PubKeyType	PubKeyBits	Subject
7834056af327e698562276902b9	12	0	?	?	?	?	?	?	Compliant	9	7834056af327e698562276902b9	04/22/2015	12/22/2041		SHA384withECDSA	EC	384	CN=Apple, Inc., CN=Apple
783ded454912d020652c83de30b55b134de859	6	0	?	?	?	?	?	?	Compliant	9	783ded454912d020652c83de30b55b134de859	10/27/2020	10/22/2040		SHA384withECDSA	EC	384	CN=SE Secure Boot Root CA Loca
785663d6d61379d4b4d6ad5517dcbf	31	0	?	?	?	?	?	?	Compliant	9	785663d6d61379d4b4d6ad5517dcbf	08/21/2019	08/21/2044		SHA384withRSA	EC	4096	CN=US, O=Apple Inc., CN=Apple
78585f2ead2c194be3370735341328b596d46593	110	0	?	?	?	?	?	?	Compliant	9	78585f2ead2c194be3370735341328b596d46593	01/12/2012	01/12/2042		SHA256withRSA	RSA	4096	CN=QuoVadis Root CA 1 G3, O=
78585f2ead2c194be3370735341328b596d46593	2	0	?	?	?	?	?	?	Compliant	9	78585f2ead2c194be3370735341328b596d46593	01/12/2012	01/12/2042		SHA256withRSA	RSA	4096	CN=QuoVadis Root CA 1 G3, O=
786c7c59fc7ca0c0	2	0	?	?	?	?	?	?	Compliant	9	786c7c59fc7ca0c0	05/17/2018	11/12/2028		SHA256withRSA	RSA	4096	CN=Digitigity BV PKiverheid C
788275c81125220a50402d4ddba73f4	64	0	?	?	?	?	?	?	Compliant	9	788275c81125220a50402d4ddba73f4	03/26/2018	03/26/2043		SHA384withECDSA	EC	384	CN=Certum Public CA, OU=Cert
78a33559c08ec9e85b571d27b22e	4	0	?	?	?	?	?	?	Compliant	9	78a33559c08ec9e85b571d27b22e	01/21/2020	01/19/2028		SHA256withRSA	RSA	4096	CN=International Hellenic Univ
78e991b38979474941e81690b20a2eae4a12a664	2	0	?	?	?	?	?	?	Compliant	9	78e991b38979474941e81690b20a2eae4a12a664	07/07/2022	07/06/2052		SHA256withECDSA	EC	256	CN=TS01-TERM-CN-E
78d8811bd670c68	2	0	?	?	?	?	?	?	Compliant	9	78d8811bd670c68	04/20/2017	03/22/2032		SHA256withECDSA	EC	256	ST=California, O=Apple Inc., CN
78d0a90d3f119e434e4ef1b0235a	4	0	?	?	?	?	?	?	Compliant	9	78d0a90d3f119e434e4ef1b0235a	05/28/2014	05/28/2039		SHA256withRSA	RSA	4096	CN=Microsoft Development Root
78d846d3b5b5817	4	0	?	?	?	?	?	?	Compliant	9	78d846d3b5b5817	04/20/2017	03/22/2032		SHA384withECDSA	EC	384	ST=California, O=Apple Inc., CN
79299b22c0f9a55e69621c7b8221b5f	2	0	?	?	?	?	?	?	Compliant	9	79299b22c0f9a55e69621c7b8221b5f	03/24/2021	03/24/2030		SHA384withECDSA	EC	384	CN=GlobalSign GCC ES EV QWA
79299b472cc752112649aa4b7c3e1e	2	0	?	?	?	?	?	?	Compliant	9	79299b472cc752112649aa4b7c3e1e	03/24/2021	03/24/2030		SHA384withECDSA	EC	384	CN=GlobalSign GCC ES EV QW
79384bb41a8d7422c0ff853f2e4ba	8	0	?	?	?	?	?	?	Compliant	9	79384bb41a8d7422c0ff853f2e4ba	11/18/2015	01/19/2038		SHA384withECDSA	EC	384	CN=Network Solutions ECC Cert
79599033de7b620156ad822ccf1a6b2	8	0	?	?	?	?	?	?	Compliant	9	79599033de7b620156ad822ccf1a6b2	03/13/2020	03/13/2030		SHA256withRSA	RSA	256	CN=DigICert Secure Site Pro EV E
79e468e42dea206860a8d08917d5c02d9523f4f	2	0	?	?	?	?	?	?	Compliant	9	79e468e42dea206860a8d08917d5c02d9523f4f	10/28/2020	10/23/2040		SHA384withECDSA	EC	384	CN=SE_S3030V-Local-ManifestK
79e492886376d40848c23fc631e663	4	0	?	?	?	?	?	?	Compliant	9	79e492886376d40848c23fc631e663	09/04/2020	09/15/2025		SHA256withRSA	EC	384	CN=ISRC Root X2, O=Internet SE
7a1189c3e6c388e	2	0	?	?	?	?	?	?	Compliant	9	7a1189c3e6c388e	10/29/2019	10/29/2119		SHA256withECDSA	EC	256	CN=SMACC-ENC-EUR-E
7a3803288a05482c6ec077c4f4a865e	4	0	?	?	?	?	?	?	Compliant	9	7a3803288a05482c6ec077c4f4a865e	06/29/2022	06/25/2037		SHA384withECDSA	EC	384	CN=HARICA Institutional TLS ECL
7a34f1e1bd42e8936bc5287a5a15599174b2f	2	0	?	?	?	?	?	?	Compliant	9	7a34f1e1bd42e8936bc5287a5a15599174b2f	07/07/2022	07/06/2052		SHA256withECDSA	EC	256	CN=TS01-P
7a4343ead226c23cd86528aa803c59	2	0	?	?	?	?	?	?	Compliant	9	7a4343ead226c23cd86528aa803c59	12/07/2022	10/19/2052		SHA256withECDSA	EC	256	CN=Lotus-APPLE-TERM-CN-P
7a46093e237cbbab4021ce1c70aa00c	6	0	?	?	?	?	?	?	Compliant	9	7a46093e237cbbab4021ce1c70aa00c	03/26/2019	03/22/2034		SHA256withRSA	RSA	4096	CN=SSL.com SSL Enterprise Inter
7a5de933d0049eb34a1a1774cb169b6d	8	0	?	?	?	?	?	?	Compliant	9	7a5de933d0049eb34a1a1774cb169b6d	03/24/2004	03/24/2029		SHA1withRSA	RSA	4096	CN=ComSign Advanced Security
7a7c7d2f4b6fc0727b23dadaebbac8	4	0	?	?	?	?	?	?	Compliant	9	7a7c7d2f4b6fc0727b23dadaebbac8	06/21/2024	01/01/2029		SHA256withRSA	RSA	4096	CN=SSL.com IV TLS Transi RSA
7a725c3800b01a241f509ba3866b2	110	0	?	?	?	?	?	?	Compliant	9	7a725c3800b01a241f509ba3866b2	08/18/2021	08/18/2031		SHA384withRSA	RSA	4096	CN=TK Elevator Atlas RS DV CA
7a85473b2eb96789f11c3531a7ae7f6e3040d	31	0	?	?	?	?	?	?	Compliant	9	7a85473b2eb96789f11c3531a7ae7f6e3040d	01/19/2023	01/16/2048		SHA384withRSA	RSA	4096	ST=California, O=Apple Inc., CN
7ad55896c745cd97090b00467d632b	6	0	?	?	?	?	?	?	Compliant	9	7ad55896c745cd97090b00467d632b	06/25/2021	06/25/2031		SHA384withECDSA	EC	256	CN=Veroyek Verified Business (E
7afid47979017da744dc5b40dc87e20	4	0	?	?	?	?	?	?	Compliant	9	7afid47979017da744dc5b40dc87e20	03/24/2020	03/22/2028		SHA256withRSA	RSA	4096	CN=Panteion Univ. of Social and

3,300 Base Certificates | Expired: 2,361 | Instances: 207,672 (Return = Show instances)

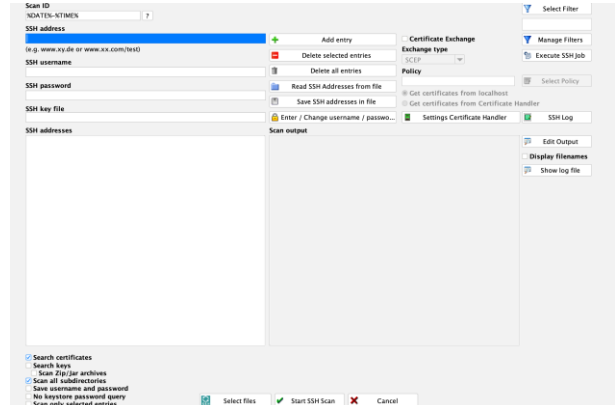
ID No.	Instances	Arch.Inst.	State	V	P	O	T	R/W	Risk Level	Priority	Serial No.	Valid from	Valid until	Revocation date	Algorithm	PubKeyType	PubKeyBits	Subject
54	104	0	?	?	?	?	?	?	Critical	9	54	05/30/2000	05/30/2020		SHA1withRSA	RSA	2048	CN=AddT
55	166	0	?	?	?	?	?	?	Medium	9	7777062726a9b17c	01/29/2010	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	66c9f990fbc039a20788a43e696365bca	05/26/2015	01/17/2038		SHA256withRSA	RSA	2048	CN=Amaz
60	94	0	?	?	?	?	?	?	Compliant	9	66c9f990fbc039a20788a43e696365bca	05/26/2015	05/26/2040		SHA384withRSA	RSA	4096	CN=Amaz
61	92	0	?	?	?	?	?	?	Compliant	9	66c9f990fbc039a20788a43e696365bca	05/26/2015	05/26/2040		SHA256withECDSA	EC	256	CN=Amaz
62	94	0	?	?	?	?	?	?	Compliant	9	66c9f990fbc039a20788a43e696365bca	05/26/2015	05/26/2040		SHA384withECDSA	EC	384	CN=Amaz
63	90	0	?	?	?	?	?	?	Medium	9	5c33cb62c5fb332	07/07/2011	01/01/2031		SHA256withRSA	RSA	2048	CN=Amaz
64	2	0	?	?	?	?	?	?	Compliant	9	1	12/22/2010	12/18/2030		SHA384withRSA	RSA	4096	CN=Amaz
65	14	0	?	?	?	?	?	?	Critical	9	3bf81d0	11/15/2000	11/10/2021		SHA1withRSA	RSA	2048	CN=Amaz
66	434	0	?	?	?	?	?	?	Medium	9	20000b9	05/12/2000	05/13/2025		SHA1withRSA	RSA	2048	CN=Amaz
67	124	0	?	?	?	?	?	?	Compliant	9	2	10/26/2010	10/26/2040		SHA256withRSA	RSA	2048	CN=Amaz
68	124	0	?	?	?	?	?	?	Compliant	9	2	10/26/2010	10/26/2040		SHA256withRSA	RSA	2048	CN=Amaz
69	42	0	?	?	?	?	?	?	Medium	9	8b5b7556845485b0d0cfaf3848ceb1a4	10/01/1999	07/17/2036		SHA1withRSA	RSA	2048	CN=Amaz
70	48	0	?	?	?	?	?	?	Medium	9	6170c498c5f984529e7b0d6d9505b7a	10/01/1999	07/17/2036		SHA1withRSA	RSA	2048	CN=Amaz
71	88	0	?	?	?	?	?	?	Medium	9	9a7e0e49a334e2b9d5ee90487129ef57	10/01/1999	07/17/2036		SHA1withRSA	RSA	2048	CN=Amaz
72	22	0	?	?	?	?	?	?	Compliant	9	039ae50906e28	07/19/2012	07/19/2042		SHA1withRSA	RSA	2048	CN=Amaz
73	90	0	?	?	?	?	?	?	Compliant	9	039ae50906e28	07/19/2012	07/19/2042		SHA1withRSA	RSA	2048	CN=Amaz
74	84	0	?	?	?	?	?	?	High	9	039ae50906e28	07/19/2012	07/19/2042		SHA1withRSA	RSA	2048	CN=Amaz
75	134	0	?	?	?	?	?	?	Medium	9	7afaa2007050544c019e9b63992a	03/06/2008	01/19/2038		SHA384withECDSA	EC	384	CN=Amaz
76	166	0	?	?	?	?	?	?	Compliant	9	4aa9fcdab636f01f74ed85b038694	01/19/2010	01/19/2038		SHA384withRSA	RSA	4096	CN=Amaz
77	158	0	?	?	?	?	?	?	Compliant	9	4aa9fcdab636f01f74ed85b038694	01/19/2010	01/19/2038		SHA384withRSA	RSA	4096	CN=Amaz
78	10	0	?	?	?	?	?	?	Compliant	9	11205583e42d3e5456852d8337b72cdc4611	05/26/2014	01/15/2038		SHA512withRSA	RSA	5120	CN=Amaz
79	10	0	?	?	?	?	?	?	Compliant	9	1120d991ceaa3e8c5e7f6902af73bc55	05/26/2014	01/15/2038		SHA384withECDSA	EC	384	CN=Amaz
80	110	0	?	?	?	?	?	?	Medium	9	fede3e10fc948ff	06/29/2007	06/29/2027		SHA1withRSA	RSA	2048	CN=Amaz
81	20	0	?	?	?	?	?	?	Compliant	9	1	10/21/2013	10/21/2033		SHA256withRSA	RSA		

# How to find them?

## Ports / Networks / Segments

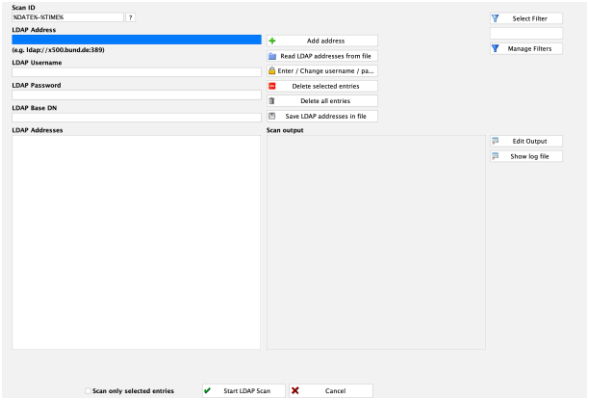


## Remote Server

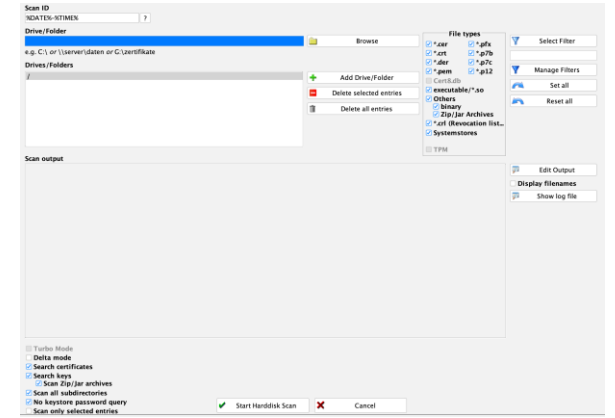


Questions asked:  
 Do you need agents?  
 Manually? Both?  
 Automated?

## Directories

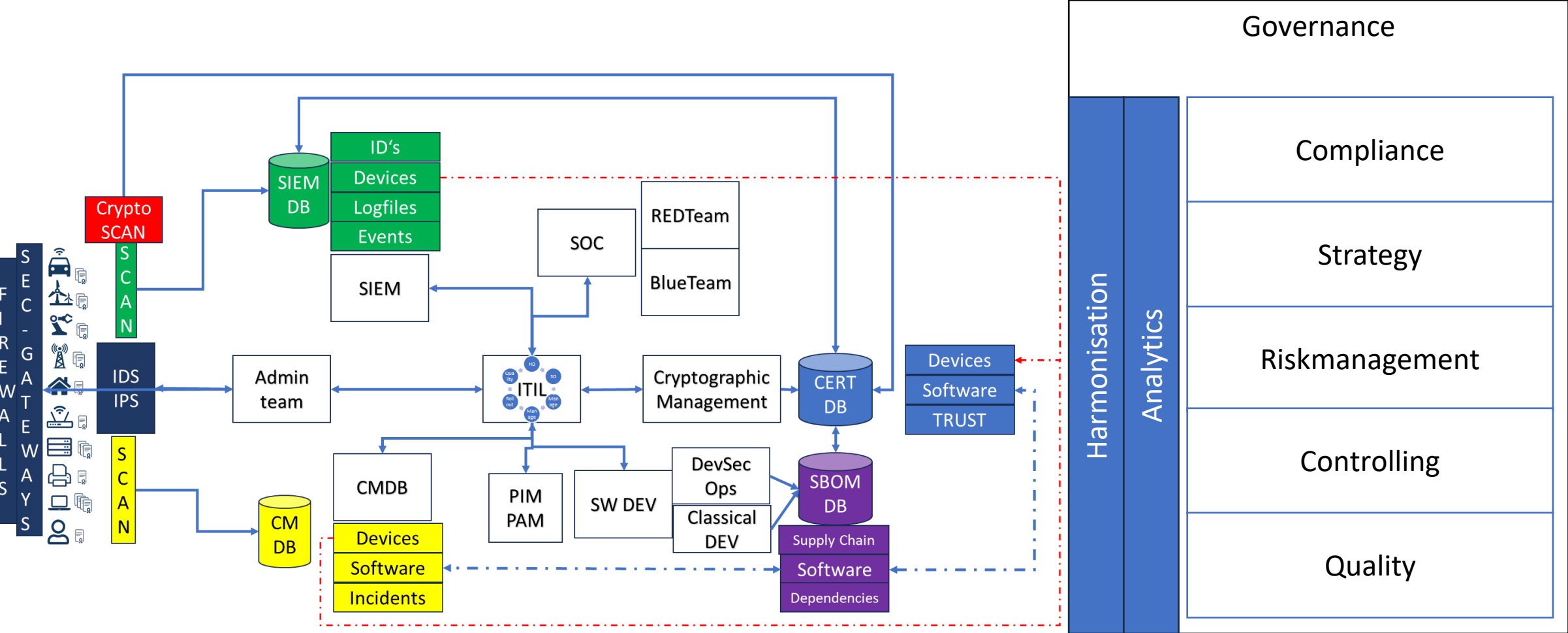


## Local

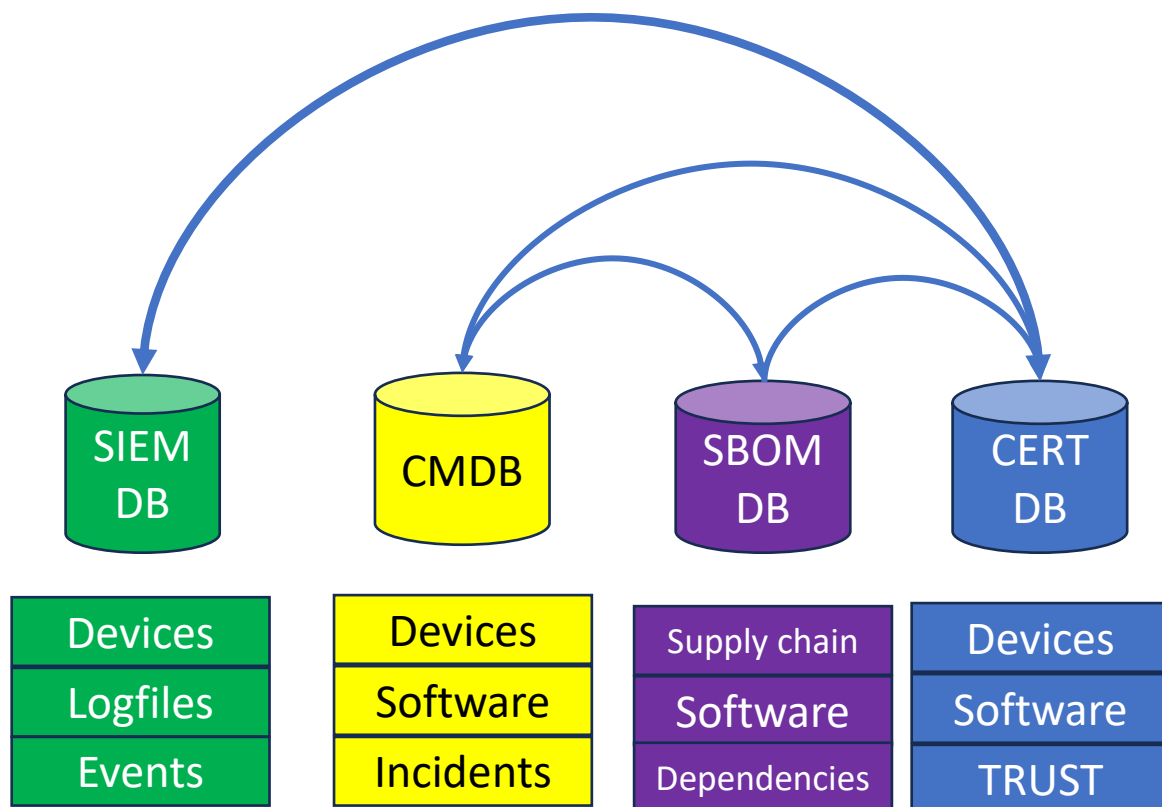


Do you ask the right questions?  
 My one would be:  
 Can you allow to miss information?  
 How can we integrate it with minimal efforts?  
 Can we support all our important processes?

# Quantum migration ready Governance



# How does Cert Discovery interface into this world and what's new?



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data
[ <!ELEMENT data (certificate+)>
  <!ELEMENT certificate (idno, certno, scandate, scantime,
origin, scanid, ipv4, ipv6, hostname, macaddress,
portpath, filename, serialno, validfrom, validuntil,
revocationdate, algorithm, pubkeytype, pubkeybits,
subject, issuer, ca, pathlength, selfsigned, fileformat,
alias, ocsf, trusted, subject_alternativenames,
thumbprint_sha1, thumbprint_sha256, certificate_pem)>
  <!ELEMENT idno (#PCDATA)>
  <!ELEMENT certno (#PCDATA)>
  <!ELEMENT scandate (#PCDATA)>
  <!ELEMENT scantime (#PCDATA)>
  <!ELEMENT origin (#PCDATA)>
  <!ELEMENT scanid (#PCDATA)>
  <!ELEMENT ipv4 (#PCDATA)>
  <!ELEMENT ipv6 (#PCDATA)>
```



# Solutions necessary and addressed



Cryptographic inventory supports:

- CBOM
  - Building a Cryptographic Bill of Material and consolidate it in enterprise context
- 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
- Risk identification and monitoring
  - Identifying risk components or suppliers in the enterprise context
- Additional services like: Investigate cryptographic security
  - Eg. Keystore security, private and public key handling

# Real world problems in enterprises

- Computer Museum support
  - Support and include also older hardware/software into the inventory
- Information superiority
  - Define the level of management and independency of operation
- Automate and enable manual or identify not performed tasks
  - Automate certificate management (CLM) / reduce outages / enhance business continuity / react faster



# Thanks for your attention

Dr. Alexander Löw (Loew)

Data-Warehouse GmbH

Ottobrunn/Germany

<https://datawh.info/en/pcert>

GE: +49 170 850 5050

PCert.com

US based company (MD) in Q1/2025

Howard County (MD), USA

offices:

Sarasota (FL), USA

Santa Monica (CA), USA

US: +1 646 821 7053