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).



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





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 ressources 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
- know your business traps, compliance and frameworks
- operate in a legal status and be able to proof it
 - be able to interface with as many as possible stakeholders
- be able to adapt to any business and technological change
 - be able to transfer the current solution and data to another platform

Automation •

• Exchangeability

- reduce manual and human interaction to a maximum within compliance

• Legality

• Strategy

- Interoperability
- Flexibility

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





Visibility challenge: Cryptographic discovery (vere construction of the security of the securi



Who is to decide which is the red one?

Cryptographic-Lifecycle-Management



Discovery engines unveils the unknown unknowns to complete your infrastructure understanding



Cryptographic inventory example



Name Yes Additional and yes yes Additional and yes	Laval	Delouitu	Carial No.	Valid from	Valid until	Baugestion data	Algorithm	Bubk ov Trees	Publicution Subject
cl. 9 4bbiologi237497111577669546667 07/02/2015 SHALWINKSA RSA 2048 Ch-Sum Microsystems, Inc.", OU-Sum Krosystems, OU-Digital ID Cass" 3 - Microsoft Software 0 4b21a64 07/22/2010 01/07/2010 SHALWINKSA RSA 2048 Ch-SuperVMI Update Not 0 4b21a64 07/22/2010 01/07/2010 SHALWINKSA RSA 2048 Ch-SuperVMI Update Not 0 45050312Kaber 1366774643 07/22/2010 SHALWINKSA RSA 2048 Ch-SuperVMI Update Not Ch-SuperVMI Update Not 0 45050312Kaber 1366774643 07/22/2010 07/22/2010 SHALWINKSA RSA 2048 Ch-SuperVSA SHALWINKSA RSA 2048 Ch-	pliant	Priority 9	5erial No. 4bab0582eb2339866580ed9d3aa27b75ed5eea2	09/16/2020	Valid until 09/14/2050	Revocation date	SHA256withECDSA	EC	256 ST=California, O=Apple Inc., CN=Apple Accessories Certification Authority – 00000003
9 9 4-0477648991383262144464208073013481 01/07/2013 9442360141545 R5A 2044 On-watchell signed apps tetritori 0 4-042786274913(c13ac6c372101bc 07/27201 944235614154 R5A 2044 On-United Taut, Co-United SL Destriching Co-Difference SL Destriching Co-DifferesL Destriching Co-Difference SL De	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 V
cl 9 4eclas/4 0/18/2010 05/22/2020 SKAL winkSA KSA 10/24 Ch-Open/WH (update Root 9 4ec/ab0/2451/stc1staces/22/306 0/13/2020 15/3/2020 SKAL winkSA KSA 10/24 Ch-Open/WH (update Root Ch-Open/WH (update Root 9 4ec/ab0/2451/stc1staces/22/306 17/3/2020 0/13/2020 SKAL winkSA KSA 10/24 Ch-Open/WH (update Root Ch-Open/WH (update Root 9 4ec/ab0/2450/x5451/stc1staces/22/306 17/3/2020 SKAL winkSA KSA 4046 Ch-Open/WH (update Root Ch-Open/WH (update Root Ch-Open/WH (update Root 9 4ec/ab0/3450/x5451/stc1staces/22/3048 0/13/2020 SKAL winkSA KSA 4046 Ch-Open/WH (update Root	ium	9	4bcd77d6899133832fc144f642c9607c501d3d61	01/01/2015	01/01/2035		SHA256withRSA	RSA	2048 CN=xpcshell signed apps test root
mn 9 44923922749514Cl 34662472076 07/2470201 05/12/2027 SNA256mithAS R5A 2046 Chemined SLD Buschaland GmbH, CoEE min 9 40264062 11/16/2010 07/18/2010	cal	9	4belae04	04/28/2010	05/02/2020		SHA1withRSA	RSA	1024 CN=OpenVPN Update Root
plant 9 4038bac 91847;6440846296720 1118/2015 91/19/2038 SNA 384embKA RA 4096 Ch-Network Solutions ELC., L-jacksomills S. L.C., L-jacksomills S. L.C., L-jacksomills S. L.C., L-jacksomills S. L.C., D-2Dig(crt, Inc., CuB) plant 9 4c1896013F164267403114647761 11/15/2021 11/15/2021 SNA 256mbKA SA 4096 Ch-Network Solutions ELC., J-D'Big(crt, Inc., CuB) plant 9 4c189013F164267404432114647761 11/15/2021 SNA 256mbKA SA 4096 Ch-TellaSonera, CuB Solutions ELC., L-Jacksomilla SJ, D-Carc(Solutions ELC., L-Jacksomilla SJ, D-C	ium	9	4be92a902784951dc13ac6ce37d230fe	02/24/2021	05/31/2027		SHA256withRSA	RSA	2048 CN=United Trust, O=United SSL Deutschland GmbH, C=DE
ch 9 4-06-64 07/28/2010 07/28/2020 SHA kunkh5A RA 2016 Ch-Dirgott Security Biology Classing WC Class 12 (Stronge State) On-Ward State State Ch-Dirgott Security Sin WC Class 12 (Stronge State) Stronge Stronge State) Stronge State)	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=F
plant 9 4-128609116abedca90116abedca90116abedca90116abedc78-83 PL/15/2022 15/15	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 incorporate
mm 9 42:bh13bbc07360.4676e51.73bd58 01/15/2015 91/18/2015 91/1	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
chl 9 4.3 02/03/2014 02	ium	9	4c2b439be6d07a60ac676e51c73bd588	01/15/2015	01/15/2025		SHA384withRSA	RSA	2048 CN=TrustSign BR Certification Authority (DV) 2, O=TrustSign Certificadora Dig. & Soluções Segurar
plant 9 4c462/at6lub/780448c412rdesy2b6 10/16/2012 SHA256withSA RSA 4096 CN-Teilscores apple (C., C)-Teilscores, Or-Fil um 4c7256a26e35778e85b2b2bbb70e8 11/02/2017 SHA256withSA RSA 2048 CHL, Owaple Inc., C-HTISTAND, Dipter MVZ um 4c7256a26e35778e85b2b2bbb70e8 11/02/2017 SHA256withSA RSA 2048 CHL, Owaple Inc., C-HTISTAND, MICHTISTAND, Dipter MUZ um 4c6a3136b634055a2b754 (HTFSac24 02/11/2024 2/11/2024 SHA256withSA RSA 2048 CHL, Owaple Inc., C-HTISTAND, Cole Supple Class The Dipter Intrany Certification Attenthy - C4. Cole Supple Class The Dipter Trany Certification (Filder States) Acast Transpace Intrany Certification (Filder States) Acast Transpace Intrany Certification (Filder States) Acast Transpace Intrany Certification Spring of acast Transpace Intranspace Intr	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
cal 9 45073544/49931 11/11/202 12/26/2024 SHA256/mithSA RSA 2048 C-LA, Ox-Jimestamp Signer NWC. plant 9 4507354/2015 STA256/2015 S	pliant	9	4c462af6dbfbf7804f84c17cfea972b6	10/16/2014	10/16/2032		SHA256withRSA	RSA	4096 CN=TeliaSonera Server CA v2, O=TeliaSonera, C=FI
um 9 4:72556263557825502506b7062 11/02/2027 SHA2 SwithEXA R5A 2048 Ch-Awayo05S1 TLS R5A CG L, Ou-Domain Validated SL, D-CertCaner AG, C-DE pilant 4:625363655780250 01/15/2021 12/12/2017 SHA3 SwithECDSA EC 34 Ch-Awayo05S1 TLS R5A CG L, Ou-Domain Validated SL, D-CertCaner AG, C-DE pilant 4:625363655980052835656320 01/15/2021 01/15/2021 SHA3 SwithECDSA EC 34 Ch-Awayo06S8 CG C, D-Objectr, Inc., C-LS um 4:628516961092739631590 09/18/2024 10/19/2035 SHA3 SwithEXA R5A 2048 Ch-Statuspagelo Ch-Apple Inc., C-LS pilant 4:6285169610972496319770515b0 01/19/2018 SHA3 SwithESA R5A 2048 Ch-Statuspagelo Ch-Apple Inc., C-LS pilant 4:621502260016100000 01/19/2018 SHA1 withESA R5A 1026 Ch-TEME ACO LA 2022 AND APPLE FairFay, C-Apple Inc., C-LS quart 4:41702104000011000001 01/19/2018 SHA1 withESA R5A 1026 Ch-TEME ACO LA 2022 AND APPLE FairFay, C-Apple Inc., C-LS quart 4:417021040000110000001 01/19/2018 SHA1 withE	cal	9	4c50f334ad4d9931	11/14/2024	12/26/2024		SHA256withRSA	RSA	2048 C=US, O=Apple Inc., CN=Timestamp Signer NWK2
plant 9 4c73b553282c751164/5594409102de 10/18/2012 12/02/2037 SHA38withECDSA EC 344 CN-symance Casts 3 Public Primary Certification Authority – C4, OL-Symantee: Trust Network, EC plant 9 4c8513146365945282751414555240 01/15/2021 <td>ium</td> <td>9</td> <td>4c7256a2663e5578e85bd2b6bb70c82</td> <td>11/02/2017</td> <td>11/02/2027</td> <td></td> <td>SHA256withRSA</td> <td>RSA</td> <td>2048 CN=AlwaysOnSSL TLS RSA CA G1, OU=Domain Validated SSL, O=CertCenter AG, C=DE</td>	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
plant 9 c4ca631406381052db7614fb3b2cd 02/19/2021 02/19/2021 SHA384withECSA EC 384 OH-HARCAccde Signing ECC Root CA 2021, O-Hellenic Academic and Research Institutions CA 0 4ca8251096109b27386c3100 05/13/202 10/13/2021 SHA384withESA FSA 2046 CHStatuspage.io C	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=
plant 9 4-d8fC038346495820683266320 01/15/2021 01/15/2045 SRA 4096 CN-J00[cert. Clert. R5A/059 Root. C5, 0="Dig[Cert. Inc.", C=US cal 9 4-cal2B19561002748613777051b0 09/18/204 10/19/2025 SHA256withSA RSA 2048 CH3, 0=Apple Mac OS Application Signing cal 9 4-calF30533600014000000 03/31/2025 03/31/2020 SHA38withSA RSA 4096 CN-COMDOR DSA Certification Authority, 0=CCMDORO DAD0002.OL -Apple FairRay, 0-Apple Inc., C-US cal 9 4-cal700233600014000001 02/10/2017 02/11/2022 SHA1WithSA RSA 1024 CN-CordESA CAR/16033AM0001A000001, OU-Apple FairRay, 0-Apple Inc., C-US cal 9 4-cal700223400014000001 03/13/202 SHA1WithSA RSA 1024 CN-ErroRSUGA CAR/16033AM0001, OU-Apple FairRay, 0-Apple Inc., C-US cal 9 4-cal200231400011000001 03/13/202 SHA1WithSA RSA 1024 CN-ErroRSUGA CAR/16033AM0001, OU-Apple FairRay, 0-Apple Inc., C-US SHA1WithSA RSA 1024 CN-ErroRSUGA CAR/20001, OU-Apple FairRay, 0-Apple Inc., C-US SHA1WithSA RSA 1024 CN-ErroRSUGA CAR/200313AF0	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,
um 9 4ca28599610952795610b 09/18/2024 10/19/2025 SHA256withSA RSA 2048 CH-Statuspage Io plant 9 4ca8772458377 01/07/2016 20/07/2023 SHA256withSA RSA 2048 CH-Statuspage Io Coll Coll Coll Coll Coll Coll Coll Coll	pliant	9	4c8fc03a854eb98a09b02883c66a3c0	01/15/2021	01/15/2046		SHA384withRSA	RSA	4096 CN=DigiCert Client RSA4096 Root G5, O="DigiCert, Inc.", C=US
cal 9 4ca82r377 01/07/2016 02/07/2023 SHA256withSA RSA 2048 CclS, O-Apple Mac, CX, Apple Tac, C, N-Apple Mac, CX, Apple Mac, CX,	ium	9	4ca28f3bf96109b27d9a6197b7051bb	09/18/2024	10/19/2025		SHA256withRSA	RSA	2048 CN=*.statuspage.jo
9 4ca39ca4bc366014774ed85b03669d 01/19/2010 01/19/2018 SHA384with5A RSA 4096 CM=COMODO RSA Certification Authority, O=CMDOD CA Limited, L=Salford, ST=Creater Manc cil 9 4ca150232400014000002 03/31/210 SHA184with5A RSA 1024 CM=CmeStSD 4476103347000147000002, OU-Apple FairPlay, O=Apple Inc., C=US cil 9 4ca1702214000147000001 02/21/2102 SHA184with5A RSA 1024 CM=CmeStSD 44761033347000147000001, OU-Apple FairPlay, O=Apple Inc., C=US cil 9 4ca17022140014700001 02/21/2102 SHA184with5A RSA 1024 CM=CPMEdiaFML4CAF1902224F0014700001, OU-Apple FairPlay, O-Apple Inc., C=US cil 9 4ca72001347000101 02/21/2102 SHA184with5A RSA 1024 CM=S000147000001, OU-Apple FairPlay, O-Apple Inc., C=US vil 9 4ca72012340014000001 01/9/2/22 03/31/202 SHA184with5A RSA 1024 CM=S000147000001, OU-Apple FairPlay, O-Apple Inc., C=US vil 9 4ca720123400147000001 03/29/202 03/31/202 SHA184with5A RSA 1024 CM=S0001470000001, OU-Apple FairPlay, O-Apple Inc., C=US	cal	9	4ca81f77d5e33f7	01/07/2016	02/07/2023		SHA256withRSA	RSA	2048 C=US, O=Apple Inc., CN=Apple Mac OS Application Signing
cil 9 4cil:5032:sh001af00000 03/31/2015 03/31/2020 SHALWithSA RSA 10/2 CN=T05032:Sh000000, OU-Apple FairPlay, O-Apple Inc., C-US cil 9 4cil:50332:0001af000001 02/10/2017 02/11/2022 SHALWithSA RSA 10/2 CN=T000002, OU-Apple FairPlay, O-Apple Inc., C-US cil 9 4cil:5023:00001af000001 02/10/2017 02/11/2022 SHALWithSA RSA 10/2 CN=T000002, OU-Apple FairPlay, O-Apple Inc., C-US 9 4cil:2022:10001af000001 03/13/200 03/14/2025 SHALWithSA RSA 10/2 CN=T00001, OU-Apple FairPlay, O-Apple Inc., C-US 9 4cil:2023:af0001af000001 03/05/2021 02/04/2026 SHALWithSA RSA 10/2 CN=T000001, OU-Apple FairPlay, O-Apple Inc., C-US 9 4cil:2023:af0001af000001 02/03/2021 02/04/2026 SHALWithSA RSA 10/2 CN=T00001, OU-Apple FairPlay, O-Apple Inc., C-US cil 9 4cil:2023:af0001af000001 00/apple FairPlay, O-Apple Inc., C-US SHALWithSA RSA 10/2 CN=T0001AF000001, OU-Apple FairPlay, O-Apple Inc., C-US cil 9 4cil:2023:af001af000001 00/apple:airPlay, O-Apple Inc., C-US <td< td=""><td>pliant</td><td>9</td><td>4caaf9cadb636fe01ff74ed85b03869d</td><td>01/19/2010</td><td>01/19/2038</td><td></td><td>SHA384withRSA</td><td>RSA</td><td>4096 CN=COMODO RSA Certification Authority. O=COMODO CA Limited, L=Salford, ST=Greater Manches</td></td<>	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 Manches
cill 9 4caff20303afb001afb000002 03/04/2016 03/05/2021 SHALWithSA RSA 1024 CN-CoreLSG032Afb001afb000001 02/10/2017 22/11/2022 SHALWithSA RSA 1024 CN-CoreLSG032Afb001afb00001 02/10/2017 22/11/2022 SHALWithSA RSA 1024 CN-EFFSubCoreAdediaPEM 4CAF19022AFb001Afb00001, OU-Apple FairPily, O-Apple Inc., C-US 9 4caf201221afb001afb00001 03/13/2020 03/14/2025 SHALWithSA RSA 1024 CN-EFFSubCoreAdediaPEM 4CAF19022AFb001Afb00001, OU-Apple FairPily, O-Apple Inc., C-US 9 4caf201221afb001afb00001 02/03/10210 03/14/2026 SHALWithSA RSA 1024 CN-EfFSubCoreAdediaPEM 4CAF210223Afb001AFb00001, OU-Apple FairPily, O-Apple Inc., C-US SHALWithSA RSA 1024 CN-EfFSubCoreAdediaPEM 4CAF21023Afb001Afb00001, OU-Apple FairPily, O-Apple Inc., C-US SHALWithSA RSA 1024 CN-EfFSubCoreAdediaPEM 4CAF21023Afb001Afb00001, OU-Apple FairPily, O-Apple Inc., C-US SHALWithSA RSA 1024 CN-EfFSubCoreAdediaPEM 4CAF21023Afb001Afb00001, OU-Apple FairPily, O-Apple Inc., C-US SHALWithSA RSA 1024 CN-EfFSubCoreAdediaPEM 4CAF21023Afb001Afb00001, OU-Apple FairPily, O-Apple Inc., C-US SHALWithSA RSA 1024 CN-EfFSubCoreAdediaPEM 4CAF21023Afbb01Afbb0001, OU-Apple FairPily, O-Apple Inc.	cal	9	4caf150325af0001af00000	03/31/2015	03/31/2020		SHA1withRSA	RSA	1024 CN=iTunes.4CAF150325AF0001AF00000. QU=Apple FairPlay. Q=Apple Inc., C=US
cil 9 4c1702104f0001af000001 02/10/2017 02/11/2022 SHAI withBSA RSA 1024 CN=PFbu6crowellaPM.4C4F10221040001.0U-Apple FairPlay, O-Apple Inc., C-US 9 4ca7200313af0001af000001 03/13/2020 03/14/2025 SHAI withBSA RSA 1024 CN=PFbu6crowellaPM.4C4F1020224F0001Af000001, UU-Apple FairPlay, O-Apple Inc., C-US 9 4ca7200313af0001af000001 01/05/202 03/14/2025 SHAI withBSA RSA 1024 CN=StorAgemISub.4ca721023Af0001Af000001, UU-Apple FairPlay, O-Apple Inc., C-US 9 4ca7202329af0001af000001 03/29/2022 03/14/2025 SHAI withBSA RSA 1024 CN=Botx.4C4721023Af0001Af000001, UU-Apple FairPlay, O-Apple Inc., C-US Sta1 0 4ca7202329af0001af000001 03/29/2022 03/13/2027 SHAI withBSA RSA 1024 CN=Botx.4C47421023Af0001Af000001, UU-Apple FairPlay, O-Apple Inc., C-US 0 4ca7342162847001Af000001 03/129/2022 05/14/2016 SHAI withSSA RSA 1024 CN=Botx.4C47420234840001Af000001, UU-Apple FairPlay, O-Apple Inc., C-US Sta1 Sta1 <td>cal</td> <td>9</td> <td>4caf160303af0001af000002</td> <td>03/04/2016</td> <td>03/05/2021</td> <td></td> <td>SHA1withRSA</td> <td>RSA</td> <td>1024 CN=CoreLSKD.4CAF160303AF0001AF000002. OU=Apple FairPlay. O=Apple Inc., C=US</td>	cal	9	4caf160303af0001af000002	03/04/2016	03/05/2021		SHA1withRSA	RSA	1024 CN=CoreLSKD.4CAF160303AF0001AF000002. OU=Apple FairPlay. O=Apple Inc., C=US
c1 9 4ca190322ar0001ar000001 02/23/2019 92/24/2024 SHA1withSA RSA 1024 CN=PSPUbCoreMediaPPM 4CAF190222AF0001AF000001, 0U-Apple FairPlay, O-Apple Inc, C-US y 4ca20013120001af000001 01/13/2000 SHA1withSA RSA 1024 CN=PSPubCoreMediaPPM 4CAF190222AF0001AF000001, 0U-Apple FairPlay, O-Apple Inc, C-US y 4ca201031af000101 02/03/2021 02/03/2020 SHA1withSA RSA 1024 CN=StoreAgenStub Aca201221af0001AF000001, OU-Apple FairPlay, O-Apple Inc, C-US y 4ca21023329af0001af000001 03/29/2022 03/0/2027 SHA1withSA RSA 1024 CN=Tunes 4CAF210033Af001AF000001, OU-Apple FairPlay, O-Apple Inc, C-US Sta1withSA RSA 1024 CN=Tunes 4CAF21003Af0001AF000001, OU-Apple FairPlay, O-Apple Inc, C-US Sta1withSA RSA 1024 CN=Tunes 4CAF21003Af0001AF000001, OU-Apple FairPlay, O-Apple Inc, C-US Sta1withSA RSA 1024 CN=Tunes 4CAF21003Af001AF000001, OU-Apple FairPlay, O-Apple Inc, C-US Sta1withSA RSA 1024 CN=Tunes 4CAF21002Af001AF000001, OU-Apple FairPlay, O-Apple Inc, C-US Sta1withSA RSA 1024 CN=Tunes 4CAF21002Af001AF000001, OU-Apple FairPlay, O-Apple Inc, C-US Sta1withSA RSA 1024 CN=Tunes 4CAF21002Af001AF000001, 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
9 4-ca20031340001af000001 03/13/2020 03/14/2025 SHAL withRSA RSA 1024 CN-MobileInstallation.4C4220313AF0001AF000001.0U-Apple FairPay, O-Apple Inc., C=US 9 4-ca201020a0001af000001 01/05/2021 01/06/2026 SHAL withRSA RSA 1024 CN-StoreAgenStub Aca201221af0001af000001, OU-Apple FairPay, O-Apple Inc., C=US 9 4-ca212023040001af000001 02/03/2021 02/04/2026 SHAL withRSA RSA 1024 CN-StoreAgenStub Aca201222034F0001AF0000001, OU-Apple FairPay, O-Apple Inc., C=US 10 4-ca73421c820329Af0001af000001 03/12/2020 SHAL withRSA RSA 1024 CN-StoreAgenStub Aca20122034F0001AF0000001, OU-Apple FairPay, O-Apple Inc., C=US 10 4-ca73421c820329Af0001af000001 03/13/2027 SHAL withRSA RSA 1024 CN-StoreAgenStub Aca20122034F0001AF000001, OU-Apple FairPay, O-Apple Inc., C=US 10 4-ca73421c820329Af0001af000001 03/12/2020 SHAL withRSA RSA 1024 CN-StoreAgenStub Aca20122034F0001AF000001, OU-Apple FairPay, O-Apple Inc., C=US 10 4-ca73421c8405412 08/17/2010 8/17/2016 SHAL withRSA RSA 1024 CN-StoreAgenStub Aca20122034F001AF0000001, OU-Apple FairPay, O-Apple Inc., C=US 10 4-dc120534085126402	cal	9	4caf190222af0001af000001	02/23/2019	02/24/2024		SHA1withRSA	RSA	1024 CN=EPStubCoreMediaPEM.4CAF190222AF0001AF000001, OU=Apple FairPlay. O=Apple Inc., C=US
9 4caf201221af0001af000001 01/05/2021 01/06/2026 SHA1withRSA RSA 1024 CN=StoreAgen5tub.4caf201221af0001af000001, OU-Apple FairPlay, O-Apple Inc., C=US 9 4caf20123240001af000001 02/03/2020 02/04/2026 SHA1withRSA RSA 1024 CN=StoreAgen5tub.4caf201221af0001af000001, OU-Apple FairPlay, O-Apple Inc., C=US 9 4caf20123240001af00001 03/29/2020 SHA1withRSA RSA 1024 CN=StoreAgen5tub.4caf201221af0001af000001, OU-Apple FairPlay, O-Apple Inc., C=US cal 9 4caf20132340001af000010 00/14/2016 SHA1withRSA RSA 4096 C=TR, O=E8C Billsim Teknolojileri ve Hizmetteri AS, CN=E8C Electronik Sertifika Hizmet Sagla um 9 4cd3856bae71d09310f303a899192 05/12/12024 SHA1withRSA RSA 2048 CN=TMESTAMPS-SHA256-2019-10-15, O=DiglCert, Inc., C=US um 9 4cd20356476c51b5067160ca76d 10/01/2019 10/17/2020 SHA1withRSA RSA 2048 CN=TMESTAMPS-SHA256-2019-10-15, O=DiglCert, Inc., C=US plant 9 4d2a05476c51b5057d10401 11/05/2020 12/11/2020 SHA1withRSA RSA 2048 CN=CON SHA120001<	h	9	4caf200313af0001af000001	03/13/2020	03/14/2025		SHA1withRSA	RSA	1024 CN=MobileInstallation 4CAF200313AF0001AF000001_0LI=Apple FairPlay. Q=Apple Inc. C=US
9 4caf210203af0001af000001 02/03/2021 02/04/2026 SHA1withRSA RSA 1024 CN=iBooks.4CAF210203Af0001Af000001, OU=Apple Fairflay, O=Apple Inc., C=US 9 4caf273221264702 03/29/2022 03/30/2027 SHA1withRSA RSA 1024 CN=iTunes, 4CAF220329Af0001Af000001, OU=Apple Fairflay, O=Apple Inc., C=US 9 4caf73321267402 08/17/206 08/14/2016 SHA1withRSA RSA 1024 CN=iTunes, 4CAF220329Af0001Af000001, OU=Apple Fairflay, O=Apple Inc., C=US 9 4caf73321267402 08/17/206 08/14/2016 SHA1withRSA RSA 1024 CN=iTunes, 4CAF23023Af0001Af000001, OU=Apple Fairflay, O=Apple Inc., C=US 9 4cd7304216276150057061050731005ca764 10/01/2019 10/17/2030 SHA256withRSA RSA 2048 CN=cdnina University TLS RSA SubCA R1, O=Hellenic Academic and Research Institutions CA, C cal 4d264364770666b31310001c6791d0c1 11/05/209 12/11/2010 SHA256withRSA RSA 2048 CN=cdn, D=Timestamp Signer MA2 cal 4d56230862420Cd6d507e244dc9c 02/8/202 SHA256withRSA RSA 2048 CN=cdn, D=Timestamp Signer MA2 cal 4d56230840700 07/21/2021 09/10/2021 SHA256withRSA		9	4caf201221af0001af000001	01/05/2021	01/06/2026		SHA1withRSA	RSA	1024 CN=StoreAgentStub.4caf201221af00001af000001. QU=Apple FairPlay. Q=Apple Inc. C=US
9 4cdf220329af0001af0000001 03/29/2022 03/30/2027 SHA1withRSA RSA 1024 CN=Tunes.4CAF220329AF0001AF000001, OU=Apple FairPlay, O=Apple Inc., C=US 1 9 4cdf73421c6e7402 08/117/2006 08/14/2016 SHA1withRSA RSA 4096 C=TR, O=EBG Bilsim Teknolojileri ve Hizmetier A.S., OU=CUS Setting FairPlay, O=Apple Inc., C=US 1 9 4cdf2a95474921083d3a899192 05/18/198 08/02/2028 SHA1withRSA RSA 2048 CN=Trust Network, OU=C) SUS C=US 1 9 4cdf2a95474210d42a46046801ad76 03/22/2028 SHA256withRSA RSA 2048 CN=chniab University TLS RSA SubCA R1, O=Hellenc Cademic and Research Institutions CA. C 1 9 4d5d96030057d1001c6791d0c1 11/05/2009 12/11/2010 SHA1withRSA RSA 2048 CN=chniab University TLS RSA SubCA R1, O=Hellenc Cademic and Research Institutions CA. C 1 4d5d96030ad9c700 07/21/2011 SHA256withRSA RSA 2048 C=US, O=Apple Inc., C=US 1 4d569cca003660ed07b6td36cd990056f82e0 03/07/203 SHA256withCDSA EC 236 C=C_256 CN=COL=TEME-CN=P 4d58/25408b234056c186253224b6c3402 20/22/2020 SHA256withRSA		9	4caf210203af0001af000001	02/03/2021	02/04/2026		SHA1withRSA	RSA	1024 CN=iBooks 4CAF210203AF0001AF000001 OLI=Apple FairPlay. O=Apple Inc. C=IIS
cal 9 4cal73421c8e7402 08/17/2006 08/17/2006 08/17/2006 08/17/2006 08/17/2006 08/17/2006 08/17/2007 <	i.	9	4caf220329af0001af000001	03/29/2022	03/30/2027		SHA1withRSA	RSA	1024 CN_iTunes 4CAF220329AF0001AF000001 OIL_Annle FairPlay O_Annle Inc. C=IS
4 4 4 6 4 6 6 1024 0U=VeriSign Trust Network, 0U="(c) 1998 VeriSign, Inc For authorized use only", 0U=Class 1 9 4 4 1001 1017/2030 SHA1withRSA RSA 2048 CN=TIMESTAMP-SHA256-219-10-15, O=DiglCert, Inc.", C=US 1 9 441200524765030b574d1d5dba3555eac7 08/23/2024 SHA256withRSA RSA 2048 CN=cdni.live.ledger.com 1 9 442d3364d7e1c0da2a46046801adf36 03/24/2020 03/22/2028 SHA256withRSA RSA 4096 CN=lonian University TLS RSA SubCA R1, O=Hellenic Academic and Research Institutions CA, C cal 9 445d8030ad9c700 07/21/2021 09/01/2021 SHA256withRSA RSA 2048 C=US, O=Apple Inc., O=Timestamp Signer MA2 cal 9 445d8030ad9c700 07/21/2021 09/01/2021 SHA256withRSA RSA 2048 C=US, O=Apple Inc., N=Timestamp Signer MA2 cal 9 445d8030ad9c70 03/1/2011 02/08/2020 SHA1withRSA RSA 2048 C=US, O=Apple Inc., N=Timestamp Signer MA2 cal 9 4d5180230460762404d506264900056f82e09 03/10/2021 SHA1withRSA	cal	9	4caf73421c8e7402	08/17/2006	08/14/2016		SHA1withRSA	RSA	4096 C=TR, O=ERG Rilisim Teknolojileri ve Hizmetleri A.S., CN=ERG Elektronik Sertifika Hizmet Sačlavici
4 4 4 10		9	4cc7eaaa983e71d39310f83d3a899192	05/18/1998	08/02/2028		SHA1withRSA	RSA	1024 Oll=VeriSign Trust Network Oll="(c) 1998 VeriSign Inc. – For authorized use only" Oll=Class 1 P
cal 9 4d1c00c5d7e503b057dd1d5dba3555eac7 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=cdn.live.ledger.com cal 9 4d5d80c30ad9c700 07/21/2021 09/01/2021 SHA256withRSA RSA 2048 CN=cdn.live.ledger.com cal 9 4d5c480c20ad6d50r244dc9c 02/00/00 22/21/2028 SHA256withRSA RSA 2048 CN=cdn.live.ledger.com cal 9 4d5c480c20ad6d50r244dc9c 02/00/00 22/8/2024 SHA256withRSA RSA 2048 CN=cdn.live.ledger.com pliant 9 4d5l7c3408b24c20cd6d50r6244dc9c 02/00/08/2020 SHA12withRSA RSA 2048 CN=cdn.live.ledger.com pliant 9 4d817ef4 03/17/2011 12/18/2065 SHA12withRSA RSA 1024 CN=opnVPN web CA 2011.0.3.17 05:25:56 UTC ip-10-203-81-10 pliant 9 4d817ef4 03/10/2011 03/14/2021 SHA184withEDSA EC 256 CN=cypetrust Japan Co., Ltd.'', C=JP	ium	9	4cd3f8568ae76c61bb0fe7160cca76d	10/01/2019	10/17/2030		SHA256withRSA	RSA	2048 CN=TIMESTAMP-SHA256-2019-10-15. Q="DigiGent_Inc.", C=US
plant 9 44233644721c042a46046801adf36 03/22/202 03/22/2028 SHA256withRSA RSA 4096 CN=lonian University TLS RSA SubCA R1, O=Hellenic Academic and Research Institutions CA, C cal 9 44dedd770666b3131d00b1c6791d0c1 11/05/2009 12/11/2010 SHA256withRSA RSA 1024 CN=Adobe Systems Incorporated, OU=Information Systems, OU=Digital ID Class 3 - Microsoft cal 9 4d560c30ad6c700 07/21/2021 09/01/2021 SHA256withRSA RSA 2048 CN=Thanker SSL CA, O=Thawte, Inc., 'C=US plant 9 4d560sec0030600ed07b6fd36cd9900c56f82e09 03/30/2023 03/29/2033 SHA256withRSA RSA 1024 CN=OpenVPN Web CA 2011.03.17 05:25:56 UTC ip-10-203-81-10 plant 9 4d817ef4 03/10/2011 03/21/2021 SHA34withECDSA EC 256 CN=openVPN Web CA 2011.03.17 05:25:56 UTC ip-10-203-81-10 plant 9 4d8247384adf51f88340f4928553224b6c48fe2 06/22/2030 SHA34withECDSA EC 384 CN=openVPN Web CA 2011.03.17 05:25:56 UTC ip-10-203-81-10 plant 9 4d8247384adf51f88340f4928553224b6c48fe2 06/22/2030 SHA384withECDSA EC 384 CN=openVPN Web CA 2011.03.17 05:25:56 UTC ip-10-203-81-1	cal	9	4d1c00c5d7e6503b057dd1d5dba3555eac7	08/23/2024	11/21/2024		SHA256withRSA	RSA	2048 CN=rdn live ledger com
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 cal 9 4d5d8030ad9c700 07/21/2021 SHA256withRSA RSA 2048 C=US, O=Apolbenc., CN=Timestamp Signer MA2 cal 9 4d5f2048b24220cd6d507e244de9ec 02/08/2020 SHA1withRSA RSA 2048 C=US, O=Apolbenc., CN=Timestamp Signer MA2 pliant 9 4d669cec0030600ed07b6fd36cd9900c56f82e09 03/30/2023 03/29/2053 SHA256withECDSA EC 256 CN=GC01-TERM-CN-P v 9 4d817ef4 03/17/2011 12/14/2021 SHA1withRSA RSA 1024 CN=MobileGo Studio, O=MobileGoStudio, L=Shenzhen, ST=Guangdong, C=CN cal 9 4d817ef4 03/10/2011 03/14/2021 SHA1withRSA RSA 1024 CN=MobileGo Studio, O=MobileGoStudio, L=Shenzhen, ST=Guangdong, C=CN cal 9 4d8a247384adf541f88340f4928553224b6c48fe2 06/22/2030 SHA384withECDSA EC 384 CN=Cybertrust Japan SureServer CA G, O="Cybertrust Japan Co., Ltd.", C=JP pliant 9 4d8a247364adf541f88340f4928553224b6c48fe	nliant	9	4d2d3364d7e1c0da2a46046801adf36	03/24/2020	03/22/2028		SHA256withRSA	RSA	4096 CN=Lonian University TIS RSA SubCA R1. Q=Hellenic Academic and Research Institutions CA. C=G
cal 9 4d5d80c30ad9c700 07/21/2021 09/01/2021 SHA256withRSA RSA 2048 C=US, O=Apple Inc., CN=Timestamp Signer MA2 cal 9 4d5f2c3408b24c20cd6d507e244dc9ec 02/08/2020 SHA256withRSA RSA 2048 C=US, O=Apple Inc., CN=Timestamp Signer MA2 pliant 9 4d69cec0030600ed07b6fd36cd9900c5fd82e09 03/30/20120 03/29/2053 SHA256withRSA RSA 2048 C=US, O=Apple Inc., CN=Timestamp Signer MA2 cal 9 4d817ef4 03/10/2011 12/18/2065 SHA1withRSA RSA 1024 CN=OpenVPN Web Z011.03.17 05:25:56 UTC ip-10-203-81-10 pliant 9 4d819b64 03/10/2011 03/14/2021 SHA384withECDSA EC 384 CN=Cybertrust Japan SureServer CA C8, 0="Cybertrust Japan Co., Ltd.", C=JP pliant 9 4d8ba7b4df9e1153e1c80dee3e6f409a 03/13/2015 12/31/2030 SHA256withRSA RSA 2048 CN=Sybertrust Japan SureServer CA 2, 0=Sectigo Limited, L=Salford, ST=Grea p 4d54b2c10d43be09409c5812d3a2b064f 11/02/2018 01/01/2031 SHA384withRSA RSA 2048 CN=Spectigo RSA C101A CA C=US cal 9 4da5acf7<	cal	9	4d4edd7706ef6b3131d00b1c6791d0c1	11/05/2009	12/11/2010		SHA1withRSA	RSA	1024 CN=Adobe Systems Incorporated Oll=Information Systems Oll=Digital ID Class 3 - Microsoft Soft
cal 9 4d57c3408b24c20cddd507e244dc9ec 07/12/1021 51/12/	cal	9	4d5d80c30ad9c700	07/21/2021	09/01/2021		SHA256withRSA	RSA	2048 C=1K 0=Annle Inc. (N=Timestam Signer MA2
pliant 9 4d669cec0030600ed07b6fd36cd9900c56f82e09 03/30/2023 03/29/2053 SHA256withECDSA EC 256 CH	cal	9	4d5f2c3408b24c20cd6d507e244dc9ec	02/08/2010	02/08/2020		SHA1withRSA	RSA	2048 CN=Thave SSI CA. O="Thave Inc." C=US
9 44817ef4 03/17/2011 12/18/2065 SHA1withRSA RSA 1024 CN=MobileGo, OU=MobileGo Studio, 0=MobileGoStudio, L=Shenzhen, ST=Guangdong, C=CN cal 9 44817ef4 03/10/2011 03/14/2021 SHA1withRSA RSA 1024 CN=MobileGo, OU=MobileGo Studio, 0=MobileGoStudio, L=Shenzhen, ST=Guangdong, C=CN pliant 9 448247384adf541f88340f4928553224b6c48fe2 06/22/2030 SHA384withECDSA EC 384 CN=OpenVPN Web CA 2011.03.17 05:25:56 UTC ip-10-203-81-10 pliant 9 4d8a7bf4f9e1153e12680dee3e6f409a 03/13/2015 12/03/2018 SHA256withRSA RSA 1024 CN=OpenVPN Web CA 2011.03.17 05:25:56 UTC ip-10-203-81-10 y 4d8a7bf4f9e1153e12680dee3e6f409a 03/13/2015 12/03/2018 SHA256withRSA RSA 2048 CN=Sectigo ECC Domain Validation SSL CA, O=UniTrust, C=CN tum 9 4d842c10d43be09409c5812d3a2b064f 11/02/2018 01/01/2031 SHA384withRSA RSA 2048 CN=Sectigo RSA Client Authentication and Secure Email CA, O=Sectigo Limited, L=Salford, ST=C cal 9 4da54fc7 04/06/2011 04/10/2021 SHA1withRSA RSA 2048 CN=OpenVPN Script Root 2011.04 cal 9 <td>nliant</td> <td>9</td> <td>4d669cec0030600ed07b6fd36cd9900c56f82e09</td> <td>03/30/2023</td> <td>03/29/2053</td> <td></td> <td>SHA256withFCDSA</td> <td>FC</td> <td>256 CN=GC01-TFRM-CN-P</td>	nliant	9	4d669cec0030600ed07b6fd36cd9900c56f82e09	03/30/2023	03/29/2053		SHA256withFCDSA	FC	256 CN=GC01-TFRM-CN-P
cal03/10/201103/14/2021SHA1withRSARSA1024CH = OpenVPN Web CA 2011.03.17 05:25:56 UTC ip -10-203-81-10pliant94d8247384adf541f88340f4928553224b6c48fe206/22/202006/22/2030SHA384withECDSAEC384CN=Cybertrust Japan SureServer CA G8, O="Cybertrust Japan Co., Ltd.", C=JPpliant94d8ba7b4df9e1153e1c80dee3e6f409a03/13/201512/03/201801/01/2031SHA384withECDSAEC256CN=Sectigo ECC Domain Validation Secure Server CA 2, O=Sectigo Limited, L=Salford, ST=Grea04d8ba7b4df9e1153e1c80dee3e6f409a03/13/201512/31/2030SHA384withRSARSA2048CN=Sectigo RSA Client Authentication and Secure Server CA 2, O=Sectigo Limited, L=Salford, ST=Grea1um94d942c10d43be09409c5812d3a2b064f11/02/201801/01/2031SHA384withRSARSA2048CN=Sectigo RSA Client Authentication and Secure Email CA, O=Sectigo Limited, L=Salford, ST=Greacal94da54fc704/06/201104/10/2021SHA18withRSARSA2048CN=OpenVPN Update Root 2011.04cal94da56a9b04/06/201104/10/2021SHA18withRSARSA1024CN=OpenVPN Script Root 2011.04cal94da56a9b04/06/201104/10/2021SHA18withRSARSA1048CN=OpenVPN Script Root 2011.04cal94da56a9b04/06/201104/10/2021SHA18withRSARSA1024CN=OpenVPN Script Root 2011.04cal94dd5a937935c7c662428d193cf607/30/201407/30/2029SHA384withRSARSA1	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
 bitattation bitattat	cal	9	4d819b64	03/10/2011	03/14/2021		SHA1withRSA	RSA	1024 CN=OpenVPN Web CA 2011 03 17 05 25 56 LTC in-10-203-81-10
 Hard Hard Hard Hard Hard Hard Hard Hard	pliant	9	4d8247384adf541f88340f4928553224b6c48fe2	06/22/2020	06/22/2030		SHA384withECDSA	FC	384 CN=Cybertrust Japan SureServer CA G8, O="Cybertrust Japan Co., Ltd." C=IP
9Ad8ba7b4df9e1153e1c80dee3e6f409a03/13/201512/13/2030SHA256withRSARSA2048CH=SHECA Extended Validation SSL CA, O=UniTrust, C=CN1um94d942c10d43be09409c5812d3a2b064f11/02/201801/01/2031SHA256withRSARSA2048CN=SHECA Extended Validation SSL CA, O=UniTrust, C=CNcal94da5fa?04/06/201104/10/2021SHA256withRSARSA2048CN=SHECA Extended Validation SSL CA, O=UniTrust, C=CNcal94da56a9b04/06/201104/10/2021SHA1withRSARSA2048CN=OpenVPN bydate Root 2011.04cal94da56a9b04/06/201104/10/2021SHA1withRSARSA2048CN=OpenVPN Script Root 2011.04pliant94dd1c6d49937935c7c662428d193cf607/30/201407/30/2029SHA384withRSARSA4096CN=NCC Group Secure Server CA G4, 0=NCC Group, C=USpliant94dd7ccd8bfa3555392fa387b478e566f03/14/201903/12/2027SHA256withRSARSA4096CN=Exclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Ecclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Ecclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Ecclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Ecclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Ecclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Ecclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Ecclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Ecclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Ecclesiastical Academy of Vella SSL RAS SubCA R2, 0=University Ecclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Eccl	nliant	9	4d8a4a1dabf126dac726fc663fab72a9	12/03/2018	01/01/2031		SHA384withFCDSA	FC	256 CN=Section FCC Domain Validation Secure Server CA 2, 0=Section Limited L=Salford ST=Greater
Image: Instruction05/22/221805/22/22	h	9	4d8ba7b4df9e1153e1c80dee3e6f409a	03/13/2015	12/31/2030		SHA256withRSA	RSA	2048 CN=SHECA Extended Validation SSL CA. O=UniTrust. C=CN
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 Update Root 2011.04 cal 9 4da56a9b 04/06/2011 04/10/2021 SHA1withRSA RSA 2048 CN=OpenVPN Script Root 2011.04 pliant 9 4dd1c6d49937935c7c662428d193cf6 07/30/2014 01/30/2029 SHA384withRSA RSA 1024 CN=JY Private Root pliant 9 4dd7ccd8bfe3555392fa387b478e566f 03/14/2019 03/12/2027 SHA256withRSA RSA 4096 CN=Ecclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Ecclesiastical Academy of 10 9 4dd7ccd8bfe3555392fa387b478e566f 03/14/2019 03/12/2027 SHA256withRSA RSA 4096 CN=Ecclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Ecclesiastical Academy of 10 9 4dd7cod8bfe32b500b516312b00894f42ee 04/29/2015 04/29/2025 SHA384withRSA RSA 2048 CN=Western Digital Technologies Certification Authority, 0=Western Digital Technologies Certification Authority, 0=Western Digital Technologies Certification Authority, 0=CN= 10 9 4df7c019184c7b610461045e95 004/20/2022 SHA384withRSA RSA 2048 CN=Western Digital Technologies Certification Authority, 0=CN= 10 40/20/20184c7b6105c41045e95 004/20/2022 SHA384withRSA RSA 2048 CN=Western Digital Technologies Certification Authority, 0=CN= 10 40/20/20184c7b6105c41045e95 004/20/2022 SHA384withRSA RSA 2048 CN=Western Digital Technologies Certification Authority, 0=CN= 10 40/2019184c7b6105c41045e95 004/20/2022 SHA384withRSA RSA 2048 CN=Western Digital Technologies Certification Authority, 0=CN= 10 40/2019184c7b6105c41045e95 004/2012015 04/201202 SHA384withRSA RSA 2048 CN=Western Digital Technologies Certification Authority, 0=CN= 10 40/2019184c7b6105c41045e95 004/2012015 04/201202 SHA384withRSA RSA 2048 CN=Western Digital Technologies Certification Authority, 0=CN= 10 40/2019184c7b6105c41045e95 004/2012015 04/201202 SHA384withRSA RSA 2048 CN=Western Digital Technologies Certification Authority, 0=CN= 10 40/2019184c7b6105c41045e950 04/201203 SHA384withRSA RSA 2048 CN=Western Digital Technologies Certification Authority, 0=Wester	ium	9	4d942c10d43be09409c5812d3a2b064f	11/02/2018	01/01/2031		SHA384withRSA	RSA	2048 CN-Section RSA Client Authentication and Secure Email CA O=Section Limited L=Salford ST=Cree
cal 9 4da54c8 04/06/2011 04/10/2021 SHAIWithON R5A 2048 CH=OpentVB Script Root 2011.04 cal 9 4da56a9b 04/06/2011 04/10/2021 SHAIWithRSA R5A 1024 CN=SpentVB Script Root 2011.04 pliant 9 4dd1c6d49937935c7c662428d193cf6 07/30/2014 07/30/2029 SHA384withRSA R5A 4096 CN=NCC Group Secure Server CA G4, 0=NCC Group, C=US pliant 9 4dd7ccd8bfe3555392fa387b478e566f 03/14/2019 03/12/2027 SHA286withRSA R5A 4096 CN=Exclesiatical Academy of Vella SSL R5A SubCA R2, 0=University Ecclesiastical Academy of tum 9 4dd7c300184c7h632b600b51d321b00894f42ee 04/20/2015 04/29/2025 SHA384withRSA R5A 2048 CN=Exclesiatical Academy of Vella SSL R5A SubCA R2, 0=University Ecclesiastical Academy of tum 9 4dd7c300184c7h632b600b51d321b00894f42ee 04/20/2022 SHA384withRSA R5A 2048 CN=Exclesiatical Academy of Vella SSL R5A Outhority, 0=Western Digital Technologies Certification Authority, 0=Certification Authority, 0=Certification Authority, 0=Certification Authority, 0=Cerification Authority, 0=	cal	ģ	4da54fc7	04/06/2011	04/10/2021		SHA1withRSA	RSA	2018 CN=OnenVPN Indate Root 2011 04
cal 9 4da56a9b 04/06/2011 04/10/2021 SHATMING RSA 1024 CH=9P Private Root pliant 9 4dd56a9b 07/30/2014 07/30/2029 SHATMING RSA 1024 CH=9P Private Root pliant 9 4dd7cd8bf63555392fa387b478e566f 03/14/2019 03/12/2027 SHA256withRSA RSA 4096 CN=NCC Group Secure Server CA G4, 0=NCC Group, C=US pliant 9 4dd7cd48bf63555392fa387b478e566f 03/14/2019 03/12/2027 SHA256withRSA RSA 4096 CN=Exclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Ecclesiastical Academy of tum 9 4dd7c043018ac7b664ad48baa006b1f321b00894f42ee 04/20/2015 04/29/2025 SHA384withRSA RSA 2046 CN=Western Digital Technologies Certification Authority, 0=Western Digital Technologies Certification Authority, 0=Western Digital Technologies, C=CN reliant 9 4df7c30134ac7b660b54ad4ad5e959 04/20/2022 SHA384withRSA RSA 2046 CN=Western Digital Technologies Certification Authority, 0=Western Digital Technologies, C=CN	cal	ģ	4da54fc8	04/06/2011	04/10/2021		SHA1withRSA	RSA	2048 CN=OpenVPN Scrint Root 2011 04
pliant 9 4dd1c6d49937935c7c662428d193cf6 07/30/2014 07/30/2029 SHA384withRSA RSA 4096 CN=Ecclesiastical Academy of Vella SSL RSA SubCA R2, 0=University Eccl	cal	9	4da56a9b	04/06/2011	04/10/2021		SHA1withRSA	RSA	1024 CN=IV Private Root
pliant 9 4dd7ecd8bf3555392fa387b478e566f 03/14/2019 03/12/2027 SHA256withRSA RSA 4096 CN=Ecclesiastical Academy of Vella SSL RSA SubCR 2, 0=University Ecclesiastical Academy of ium 9 4ddcbc4d8baa006b1f321b00894f42ee 04/29/2015 04/29/2025 SHA384withRSA RSA 2096 CN=Ecclesiastical Academy of Vella SSL RSA SubCR 2, 0=University Ecclesiastical Academy of ium 9 4ddcbc4d8baa006b1f321b00894f42ee 04/29/2015 04/29/2025 SHA384withRSA RSA 2096 CN=Ecclesiastical Academy of Vella SSL RSA SubCR 2, 0=University Ecclesiastical Academy of ium 9 4ddcbc4d8baa006b1f321b00894f42ee 04/29/2015 04/29/2025 SHA384withRSA RSA 2096 CN=Ecclesiastical Academy of Vella SSL RSA SubCR 2, 0=University Ecclesiastical Academy of ium 9 4ddcbc4d8baa06b1f321b00894f42ee 04/20/2022 SHA384withRSA RSA 2096 CN=Ecclesiastical Academy of Vella SSL RSA SubCR 2, 0=University Ecclesiastical Academy of ium 9 4ddcbc4d8baa06b1f321b00894f42ee 04/20/2022 SHA384withRSA RSA 2096 CN=Ecclesiastical Academy of Vella SSL RSA SubCR 2, 0=University Ecclesiastical Academy of ium 9 4dfcbc4d8baa06b1f321b00894f42ee 04/20/2022 SHA384withRSA RSA 2096 CN=Ecclesiastical Academy of Vella SSL RSA SubCR 2, 0=University Ecclesiastical Academy of ium 9 4dfcbc4d8baa06b1f321b00894f42ee 04/20/2022 SHA384withFCDSA FC	nliant	ģ	4dd1c6d49937935c7c662428d193cf6	07/30/2014	07/30/2020		SHA384withRSA	RSA	4096 CN=NCC Group Server CA GA Q=NCC Group C=US
ium 9 4ddcbc4d8baa006b1f321b00894f42e 04/29/2015 04/29/2025 SHA384withRSA RSA 2006 CN=Meestern Digital Technologies Certification Authority, O=Western Digital Technologies (A)	nliant	9	4dd7ecd8hfe3555392fa387h478e566f	03/14/2019	03/12/2023		SHA256withRSA	RSA	4096 CN=Ecclesiastical Academy of Vella SSL RSA SubCA R2 O=University Ecclesiastical Academy of Vella
p_{1} = p_{1} = p_{2} = p_{1} = p_{2} = p_{2	ium	ģ	4dchc4d8haa006h1f321h00894f42ee	04/29/2015	04/29/2025		SHA384withRSA	RSA	2048 CN-Western Digital Technologies Certification Authority. O-Western Digital Technologies L-Invite
	nliant	9	4df7309184c7b632b600b5d4a045e959	04/20/2022	04/20/2023		SHA384withFCDSA	FC	256 CN=Trustasia FCC OV TIS CA G3 C=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





How to find them?



Ports / Networks / Segments

Address e.g. 192.168.1.10 or 192.168.1-2.0-255 or www.li or Computer name or 145.253.180.50:1-1024,200 fe80:6d61.7b4d:18d2:40858771-1024	ma.de:1-512 0.3000-4000 or	Add address	
Addresses	5. A.		
		keed addresses from the	Y Select Filter
		Delete selected entries	
	1	Delete all entries	Y Manage Pitter
	e	Save addresses in file	
Ports 1-2014			
Scan output		Found certificates	
	Edit Scan Output	1	
	Show log file		

Remote Server



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

Directories

NDATES-STIMES ?		Y Select Filter
LDAP Address		
fe a literatio faithean dide 1880	+ Add address	Manana Eliterr
(e.g. Idap//xsoubund.se:ses)	Read LDAP addresses from file	a manage mees
	🚨 Enter / Change username / pa	
LDAP Password	Delete selected entries	
	Delete all entries	
LDAP Base DN	Save LDAP addresses in file	
LDAP Addresses	Scan output	
		F Edit Output
		Show log file

Local

and the second					
Drive/Folder			File types	1	
	👜 👘	Browse	🕑 *.cer 🛛 *.pfx	Y	Select Fil
e.g. C:\ or \\server\daten or G:\zertifikate			🖸 *.ort 🗹 *.p7b		
Drives/Folders			🕑 ".der 🛛 *.p7c	-	
1		Add Drive/Folder		Y	Manage Fi
		Delete selected entries	executable/*.so	~	Set a
	-		Others	5	Reseta
		Delete all entries	Zip/Jar Archives		
Scan output			Systemstores		
				P	Edit Outp
				Dis	play filenam
					Ebow loo
Turino Mado ☐ Data mode ⊘ Sarch cutffusas ≫ Loss de just archives					
France Install Stands and France Stands and Frances Son all half may be a set of the set of					

Do you ask the right questions?

My one would be:

Can you allow to miss information? How can we integrate it with minimal effords? Can we support all our important processes?







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, ocsp, 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 adressed



Cryptographic inventory supports:

- CBOM
 - Building a Cryptrographic 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



Dr. Alexander Löw (Loew) Data-Warehouse GmbH Ottobrunn/Germany <u>https://datawh.info/en/pcert</u>

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

GE: +49 170 850 5050