Trusted CA List

Approach

- **Baseline**: Use a proper baseline CA list (Mozilla, OpenJDK, Microsoft, Cloudflare, ...)
- **Filtering Criteria**: Remove the obvious CA's that won't be used by filtering
- **Notification**: Informing the issuers/acquirers for removing a CA from Trusted CA list

Baseline

As a baseline iDEAL 2.0 access point will use Mozilla's list of trusted root CA's, since Mozilla is known for very careful, open and elaborative assessing of trust:

- Mozilla is known as an authority, yet open, worldwide
- The process is very open: https://bugzilla.mozilla.org/show_bug.cgi?id=1668131
- As Firefox is a widely used browser, the CA list is extremely up-to-date, in comparison with Oracle's shipped truststore.
- Follow changes here: https://wiki.mozilla.org/CA/Additional_Trust_Changes
- An endless number of (open source) projects is relying on Mozilla

Filtering criteria

To limit threat surface, yet staying flexible enough in iDEAL 2.0 access point, CA list will be limited to:

- only NL, Europe-wide, global and US based CA's
- for global/europe-wide CA's:
    - only US (global), NL, BE, Luxembourg, Germany based
      Note1: that this list simply allows to rule out a lot of unexpected CA's (probably no need for a Japanese CA in this list).
      Note2: A Dutch CA is not more or less trustworthy than another one. Yet it's better to have fewer CA's on the list. Hence a list of close-by-home CA's (jurisdiction), and in addition the widely used US-based ones.
    - specific geographic scope: only 1 country + global (so not 'US,UK,Global')
- only website-type CA's (not email etc)

The criteria additionally will be applied for filtering the CA’s:

- Goto CA's for attackers (e.g. Let's encrypt, or it's root CA)
- non-NL or non-europe-wide CA's
- CA's with 'Mozilla Applied Constraints' (e.g. 3rd party auditing (WebTrust, ETSI EN 319 411)

Therefore, the below CA’s will be removed:

- Let's encrypt: too accessible and anonymous
- Sectigo: used as root for a lot of free-SSL companies

Notification

iDEAL 2.0 access point will monitor the distrust events of CA’s and will notify Currence to inform relevant parties that the trust of a CA’s will be revoked. A CA can be revoked from the Trusted CA List baseline for the following reasons:

- Coordinated / planned distrust. This happens if a CA is becoming obsolete in favor of another. Expiration date still in the future.

- CA compromise or failing audit
  Removal is a feature in this case; iDEAL 2.0 access point will follow this distrust in case of compromise.

List of Trusted CA

Common Name or Certificate Name	Certificate Serial Number	SHA-256 Fingerprint	Geographic Focus
Amazon Root CA 1	066C9FCF99BF8C0A39E2F0788A43E696365BCA	8ECDE6884F3D87B1125BA31AC3FCB13D7016DE7F57CC904FE1CB97C6AE98196E	USA, Global
Amazon Root CA 2	066C9FD29635869F0A0FE58678F85B26BB8A37	1BA5B2AA8C65401A82960118F80BEC4F62304D83CEC4713A19C39C011EA46DB4	USA, Global
Amazon Root CA 3	066C9FD5749736663F3B0B9AD9E89E7603F24A	18CE6CFE7BF14E60B2E347B8DFE868CB31D02EBB3ADA271569F50343B46DB3A4	USA, Global
Amazon Root CA 4	066C9FD7C1BB104C2943E5717B7B2CC81AC10E	E35D28419ED02025CFA69038CD623962458DA5C695FBDEA3C22B0BFB25897092	USA, Global
Starfield Services Root Certificate Authority - G2	0	568D6905A2C88708A4B3025190EDCFEDB1974A606A13C6E5290FCB2AE63EDAB5	USA, Global
Atos TrustedRoot 2011	5C33CB622C5FB332	F356BEA244B7A91EB35D53CA9AD7864ACE018E2D35D5F8F96DDF68A6F41AA474	Germany, Europe
D-TRUST Root Class 3 CA 2 2009	0983F3	49E7A442ACF0EA6287050054B52564B650E4F49E42E348D6AA38E039E957B1C1	Germany, Europe, Global
D-TRUST Root Class 3 CA 2 EV 2009	0983F4	EEC5496B988CE98625B934092EEC2908BED0B0F316C2D4730C84EAF1F3D34881	Germany, Europe, Global
Baltimore CyberTrust Root	020000B9	16AF57A9F676B0AB126095AA5EBADEF22AB31119D644AC95CD4B93DBF3F26AEB	USA, Global
Cybertrust Global Root	0400000000010F85AA2D48	960ADF0063E96356750C2965DD0A0867DA0B9CBD6E77714AEAFB2349AB393DA3	USA, Global
DigiCert Assured ID Root CA	0CE7E0E517D846FE8FE560FC1BF03039	3E9099B5015E8F486C00BCEA9D111EE721FABA355A89BCF1DF69561E3DC6325C	USA, Global
DigiCert Assured ID Root G2	0B931C3AD63967EA6723BFC3AF9AF44B	7D05EBB682339F8C9451EE094EEBFEFA7953A114EDB2F44949452FAB7D2FC185	USA, Global
DigiCert Assured ID Root G3	0BA15AFA1DDFA0B54944AFCD24A06CEC	7E37CB8B4C47090CAB36551BA6F45DB840680FBA166A952DB100717F43053FC2	USA, Global
DigiCert Global Root CA	083BE056904246B1A1756AC95991C74A	4348A0E9444C78CB265E058D5E8944B4D84F9662BD26DB257F8934A443C70161	USA, Global
DigiCert Global Root G2	033AF1E6A711A9A0BB2864B11D09FAE5	CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F	USA, Global
DigiCert Global Root G3	055556BCF25EA43535C3A40FD5AB4572	31AD6648F8104138C738F39EA4320133393E3A18CC02296EF97C2AC9EF6731D0	USA, Global
DigiCert High Assurance EV Root CA	02AC5C266A0B409B8F0B79F2AE462577	7431E5F4C3C1CE4690774F0B61E05440883BA9A01ED00BA6ABD7806ED3B118CF	USA, Global
DigiCert Trusted Root G4	059B1B579E8E2132E23907BDA777755C	552F7BDCF1A7AF9E6CE672017F4F12ABF77240C78E761AC203D1D9D20AC89988	USA, Global
AffirmTrust Commercial	7777062726A9B17C	0376AB1D54C5F9803CE4B2E201A0EE7EEF7B57B636E8A93C9B8D4860C96F5FA7	North America, Global
AffirmTrust Networking	7C4F04391CD4992D	0A81EC5A929777F145904AF38D5D509F66B5E2C58FCDB531058B0E17F3F0B41B	North America, Global
AffirmTrust Premium	6D8C1446B1A60AEE	70A73F7F376B60074248904534B11482D5BF0E698ECC498DF52577EBF2E93B9A	North America, Global
AffirmTrust Premium ECC	7497258AC73F7A54	BD71FDF6DA97E4CF62D1647ADD2581B07D79ADF8397EB4ECBA9C5E8488821423	North America, Global
Entrust Root Certification Authority	456B5054	73C176434F1BC6D5ADF45B0E76E727287C8DE57616C1E6E6141A2B2CBC7D8E4C	North America, Global
Entrust Root Certification Authority - EC1	00A68B79290000000050D091F9	02ED0EB28C14DA45165C566791700D6451D7FB56F0B2AB1D3B8EB070E56EDFF5	North America, Global
Entrust Root Certification Authority - G2	4A538C28	43DF5774B03E7FEF5FE40D931A7BEDF1BB2E6B42738C4E6D3841103D3AA7F339	North America, Global
Entrust Root Certification Authority - G4	00D9B5437FAFA9390F000000005565AD58	DB3517D1F6732A2D5AB97C533EC70779EE3270A62FB4AC4238372460E6F01E88	North America, Global
Entrust.net Certification Authority (2048)	3863DEF8	6DC47172E01CBCB0BF62580D895FE2B8AC9AD4F873801E0C10B9C837D21EB177	North America, Global
GlobalSign	0400000000121585308A2	CBB522D7B7F127AD6A0113865BDF1CD4102E7D0759AF635A7CF4720DC963C53B	Belgium, Global
GlobalSign	45E6BB038333C3856548E6FF4551	2CABEAFE37D06CA22ABA7391C0033D25982952C453647349763A3AB5AD6CCF69	Belgium, Global
GlobalSign	605949E0262EBB55F90A778A71F94AD86C	179FBC148A3DD00FD24EA13458CC43BFA7F59C8182D783A513F6EBEC100C8924	Belgium, Global
GlobalSign Root CA	040000000001154B5AC394	EBD41040E4BB3EC742C9E381D31EF2A41A48B6685C96E7CEF3C1DF6CD4331C99	Belgium, Global
GlobalSign Root E46	11D2BBBA336ED4BCE62468C50D841D98E843	CBB9C44D84B8043E1050EA31A69F514955D7BFD2E2C6B49301019AD61D9F5058	Belgium, Global
GlobalSign Root R46	11D2BBB9D723189E405F0A9D2DD0DF2567D1	4FA3126D8D3A11D1C4855A4F807CBAD6CF919D3A5A88B03BEA2C6372D93C40C9	Belgium, Global

Go Daddy Class 2 CA	0	C3846BF24B9E93CA64274C0EC67C1ECC5E024FFCACD2D74019350E81FE546AE4	USA, Global
Go Daddy Root Certificate Authority - G2	0	45140B3247EB9CC8C5B4F0D7B53091F73292089E6E5A63E2749DD3ACA9198EDA	USA, Global
Starfield Class 2 CA	0	1465FA205397B876FAA6F0A9958E5590E40FCC7FAA4FB7C2C8677521FB5FB658	USA, Global
Starfield Root Certificate Authority - G2	0	2CE1CB0BF9D2F9E102993FBE215152C3B2DD0CABDE1C68E5319B839154DBB7F5	USA, Global
GlobalSign	0400000000010F8626E60D	CA42DD41745FD0B81EB902362CF9D8BF719DA1BD1B1EFC946F5B4C99F42C1B9E	Global
GlobalSign	2A38A41C960A04DE42B228A50BE8349802	BEC94911C2955676DB6C0A550986D76E3BA005667C442C9762B4FBB773DE228C	Global
GTS Root R1	6E47A9C54B470C0DEC33D089B91CF4E1	2A575471E31340BC21581CBD2CF13E158463203ECE94BCF9D3CC196BF09A5472	Global
GTS Root R2	6E47A9C65AB3E720C5309A3F6852F26F	C45D7BB08E6D67E62E4235110B564E5F78FD92EF058C840AEA4E6455D7585C60	Global
GTS Root R3	6E47A9C76CA9732440890F0355DD8D1D	15D5B8774619EA7D54CE1CA6D0B0C403E037A917F131E8A04E1E6B7A71BABCE5	Global
GTS Root R4	6E47A9C88B94B6E8BB3B2AD8A2B2C199	71CCA5391F9E794B04802530B363E121DA8A3043BB26662FEA4DCA7FC951A4BD	Global
Staat der Nederlanden EV Root CA	0098968D	4D2491414CFE956746EC4CEFA6CF6F72E28A1329432F9D8A907AC4CB5DADC15A	Netherlands
DST Root CA X3	44AFB080D6A327BA893039862EF8406B	0687260331A72403D909F105E69BCF0D32E1BD2493FFC6D9206D11BCD6770739	USA
IdenTrust Commercial Root CA 1	0A01428000000014523C844B500000002	5D56499BE4D2E08BCFCAD08A3E38723D50503BDE706948E42F55603019E528AE	USA
IdenTrust Public Sector Root CA 1	0A01428000000014523CF467C00000002	30D0895A9A448A262091635522D1F52010B5867ACAE12C78EF958FD4F4389F2F	USA
Microsoft ECC Root Certificate Authority 2017	66F23DAF87DE8BB14AEA0C573101C2EC	358DF39D764AF9E1B766E9C972DF352EE15CFAC227AF6AD1D70E8E4A6EDCBA02	Global
Microsoft RSA Root Certificate Authority 2017	1ED397095FD8B4B347701EAABE7F45B3	C741F70F4B2A8D88BF2E71C14122EF53EF10EBA0CFA5E64CFA20F418853073E0	Global
Secure Global CA	075622A4E8D48A894DF413C8F0F8EAA5	4200F5043AC8590EBB527D209ED1503029FBCBD41CA1B506EC27F15ADE7DAC69	USA, Global
SecureTrust CA	0CF08E5C0816A5AD427FF0EB271859D0	F1C1B50AE5A20DD8030EC9F6BC24823DD367B5255759B4E71B61FCE9F7375D73	USA, Global
Trustwave Global Certification Authority	05F70E86DA49F346352EBAB2	97552015F5DDFC3C8788C006944555408894450084F100867086BC1A2BB58DC8	USA, Global
Trustwave Global ECC P256 Certification Authority	0D6A5F083F285C3E5195DF5D	945BBC825EA554F489D1FD51A73DDF2EA624AC7019A05205225C22A78CCFA8B4	USA, Global
Trustwave Global ECC P384 Certification Authority	08BD85976C9927A48068473B	55903859C8C0C3EBB8759ECE4E2557225FF5758BBD38EBD48276601E1BD58097	USA, Global
XRamp Global Certification Authority	50946CEC18EAD59C4DD597EF758FA0AD	CECDDC905099D8DADFC5B1D209B737CBE2C18CFB2C10C0FF0BCF0D3286FC1AA2	USA, Global
SSL.com EV Root Certification Authority ECC	2C299C5B16ED0595	22A2C1F7BDED704CC1E701B5F408C310880FE956B5DE2A4A44F99C873A25A7C8	USA, Global
SSL.com EV Root Certification Authority RSA R2	56B629CD34BC78F6	2E7BF16CC22485A7BBE2AA8696750761B0AE39BE3B2FE9D0CC6D4EF73491425C	USA, Global
SSL.com Root Certification Authority ECC	75E6DFCBC1685BA8	3417BB06CC6007DA1B961C920B8AB4CE3FAD820E4AA30B9ACBC4A74EBDCEBC65	USA, Global
SSL.com Root Certification Authority RSA	7B2C9BD316803299	85666A562EE0BE5CE925C1D8890A6F76A87EC16D4D7D5F29EA7419CF20123B69	USA, Global