

**Er identitet i HTTPS/TLS
i ferd med å få sin renessanse?**



HTTPS-kryptering på nett

buypass.no

buypass Bedrift Person Om

BUYPASS AS

Trygg digitalt

buypass.no

- Connection is secure
- Cookies and site data
- Site settings
- About this page

Security buypass.no

- Connection is secure
- Certificate is valid

Issued to: BUYPASS AS [NO]

Certificate Viewer: www.buypass.no

General Details

Issued To

Common Name (CN)	www.buypass.no
Organization (O)	BUYPASS AS
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	Buypass Class 3 CA 2
Organization (O)	Buypass AS-983163327
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Thursday, February 2, 2023 at 4:54:16 PM
Expires On	Sunday, February 18, 2024 at 11:59:00 PM

Fingerprints

SHA-256 Fingerprint	CE B1 89 04 D1 D3 80 E8 84 C3 98 96 70 3D 1C CD 74 2E A8 A2 DC 21 08 B8 E7 FF F4 67 FE 7C 74 FB
SHA-1 Fingerprint	AF BF A2 9D 95 76 7C 02 AD 1A E9 65 B3 7A F9 59 99 16 1B 1E

sikkerhetsfestivalen.no

presse code of conduct

SIKKERHETS FESTIVALEN

Norges største møteplass for cybersikkerhet 28. - 30. august 2023

sikkerhetsfestivalen.no

- Connection is secure
- Cookies and site data
- Site settings
- About this page

Security sikkerhetsfestivalen.no

- Connection is secure
- Certificate is valid

Issued to: sikkerhetsfestivalen.no

Certificate Viewer: sikkerhetsfestivalen.no

General Details

Issued To

Common Name (CN)	sikkerhetsfestivalen.no
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	R3
Organization (O)	Let's Encrypt
Organizational Unit (OU)	<Not Part Of Certificate>

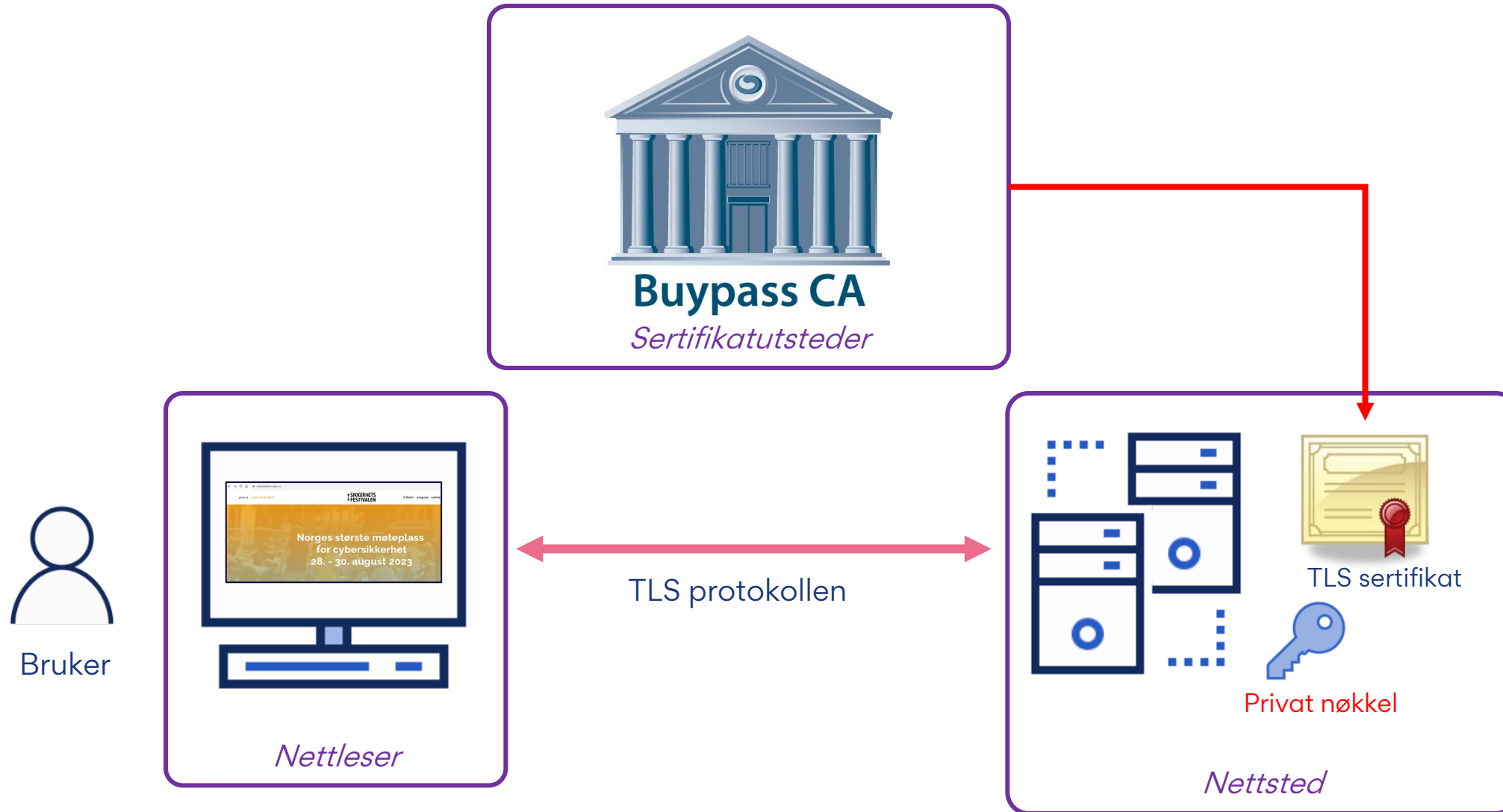
Validity Period

Issued On	Thursday, August 10, 2023 at 10:08:45 PM
Expires On	Wednesday, November 8, 2023 at 9:08:44 PM

Fingerprints

SHA-256 Fingerprint	07 18 DA 38 DB 6C CC 74 82 C6 80 9F 55 0F BE 4B 37 37 E6 2D C6 BC 9F FC 73 AC D6 17 43 0C 7E DD
SHA-1 Fingerprint	D5 69 99 FA 99 1C 64 06 16 78 2D 7D 1D 88 87 76 11 D3 4F 2E

Økosystemet rundt HTTPS/TLS



Hvorfor er HTTPS-kryptering viktig?

← → ↻ 🏠 🔒 Not secure | http.badssl.com

http.badssl.com

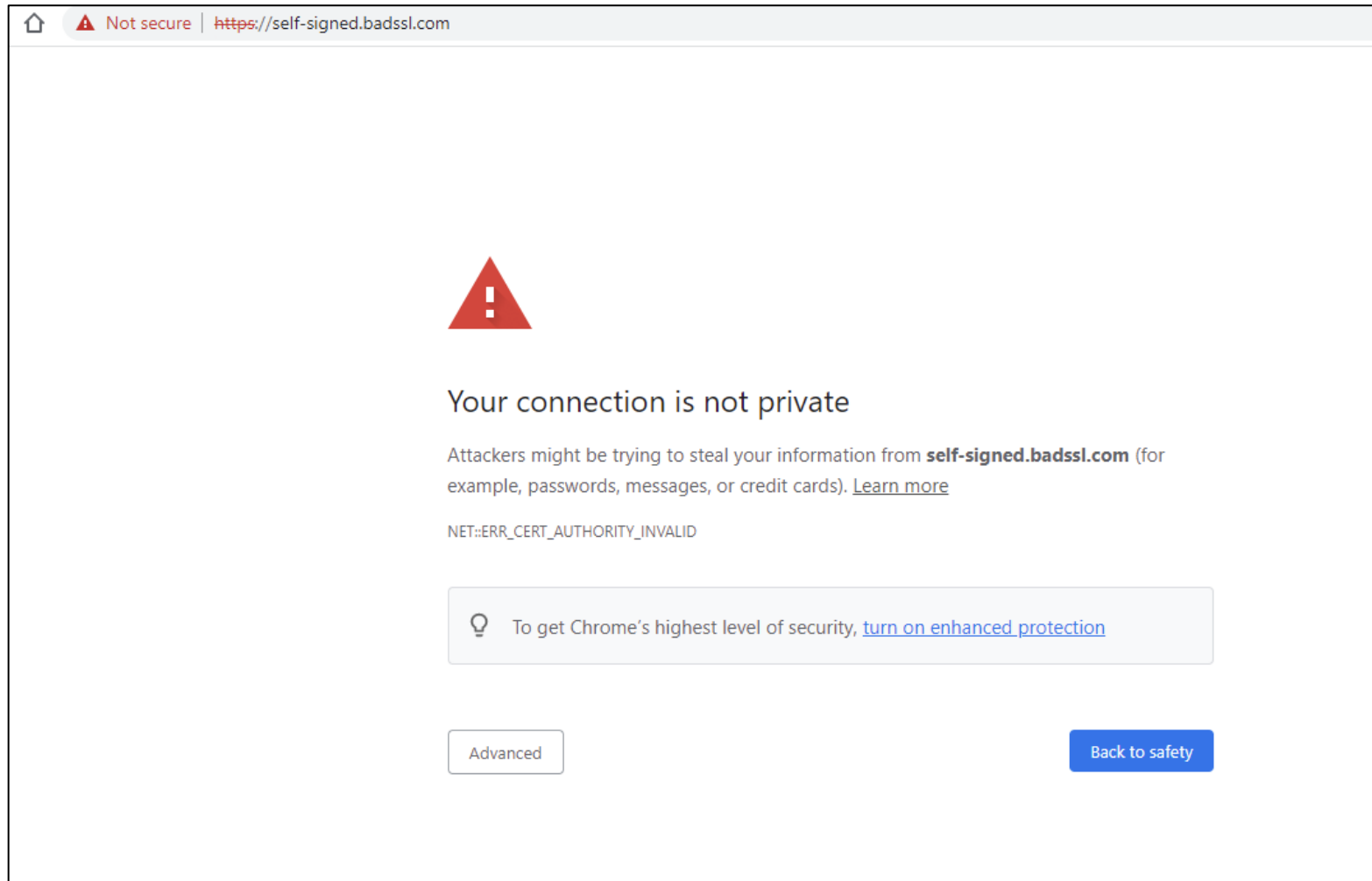
http.badssl.com

⚠️ **Your connection to this site is not secure**
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers.
[Learn more](#)

🍪 Cookies and site data ▶

⚙️ Site settings ↗

Netlesere blokkerer tilgang



Hva er HTTPS og TLS?

HTTP	FTP	SMTP
TLS		
TCP		
IP		

- TLS - Transport Layer Security
- En kryptografisk protokoll som sikrer konfidensialitet og integritet mellom to parter som kommuniserer
- Etterfølger til Secure Socket Layer (SSL)
- TLS versjoner:
 - ~~TLS v1.0 - 1998~~
 - ~~TLS v1.1 - 2003~~
 - TLS v1.2 (RFC 5246) - 2008
 - TLS v1.3 - 2018
- HTTPS: Hypertext Transfer Protocol Secure
 - HTTP over TLS

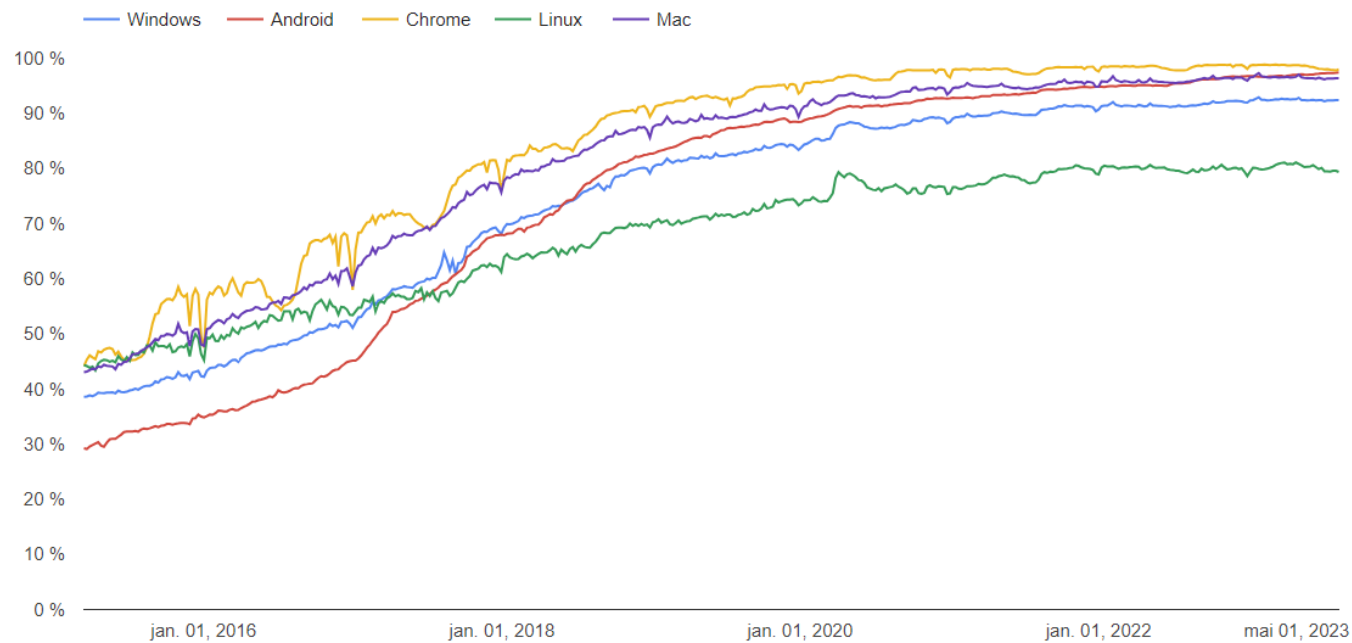


HTTPS-kryptering og bruk

HTTPS-kryptering etter Chrome-plattform

Siden begynnelsen av 2015 har vi kunnet måle utbredelsen av HTTPS-tilkoblinger, takket være Chrome-brukere som velger å [dele bruksstatistikk](#). I diagrammene nedenfor ser du økningen i HTTPS-bruk på tvers av plattformer og land/regioner. Over halvparten av sidene som åpnes av brukere på datamaskiner, lastes inn via HTTPS, og disse brukerne tilbringer to tredjedeler av internettiden sin på HTTPS-sider. HTTPS er mindre utbredt på nettsteder som åpnes på mobilenheter, men vi ser en økende trend der også.

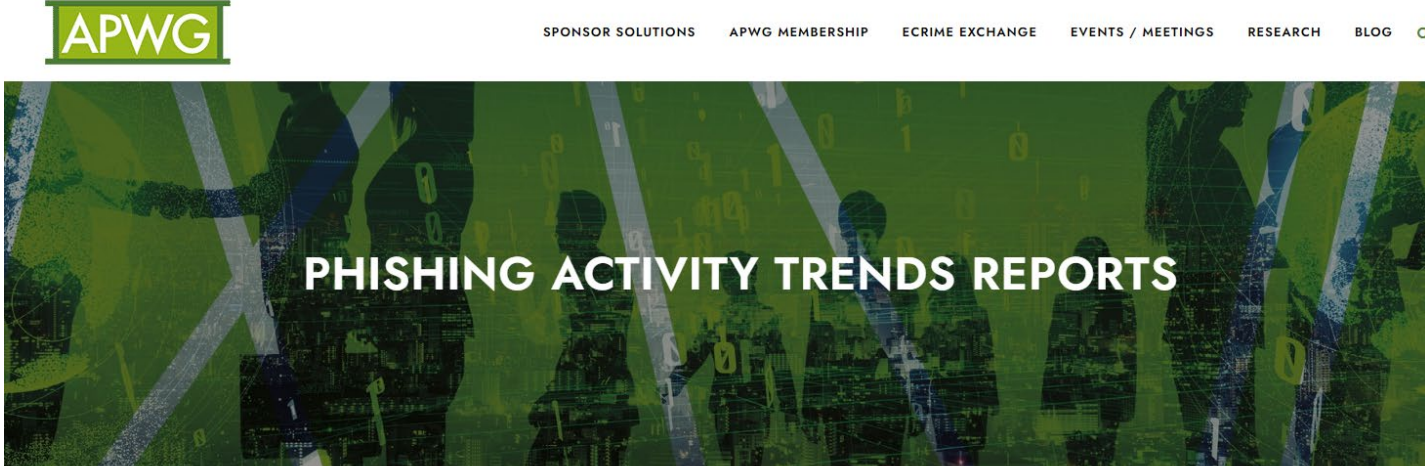
Prosentandel av sider som lastes inn via HTTPS i Chrome, etter plattform



Phising øker stadig!

På tross av HTTPS-kryptering

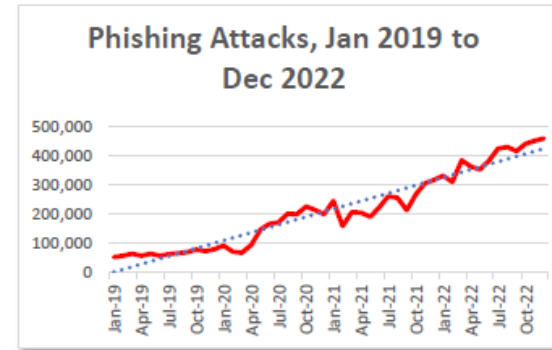
Antall phishing sites øker



PHISHING ACTIVITY TRENDS REPORTS

The APWG Phishing Activity Trends Report analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at <https://apwg.org>, and by e-mail submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation, and propagation of crimeware by d from the research of our member companies.

Phishing Reaches New Quarterly High in Late 2022

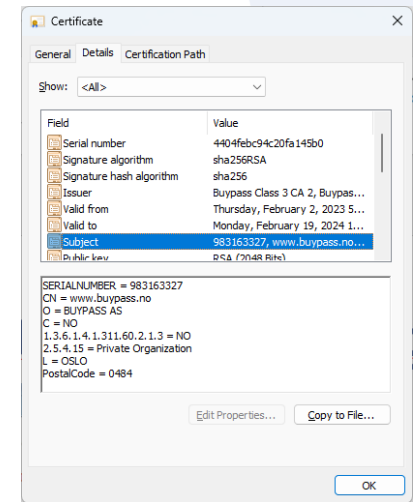
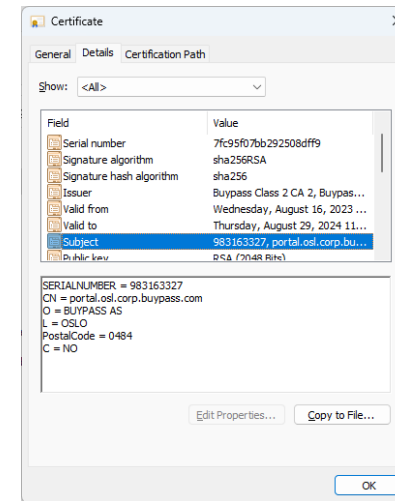
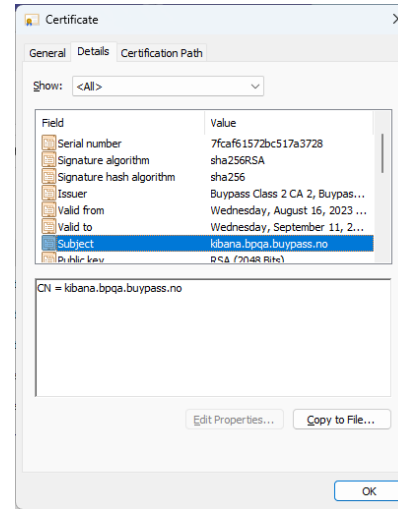


The year 2022 was another record-shattering year for phishing, with the APWG logging more than 4.7 million attacks

	October	November	December
Number of unique phishing Web sites (attacks) detected	440,508	450,390	459,139
Unique phishing email subjects	101,104	77,469	74,250
Number of brands targeted by phishing campaigns	599	610	577

Ulike typer TLS-sertifikater

- **Domenevalidert (DV)**
 - Kun kontroll på domene
- **Organisasjonsvalidert (OV)**
 - Identitet inkluderer nettstedets eier (en organisasjon)
 - Informasjon om organisasjon blir kontrollert mot offentlige registre
- **Utvidet validering (EV)**
 - Identitet inkluderer den juridiske enheten som kontrollerer nettstedet
 - Omfattende kontroller for å sikre at nettstedets eier er en operativ og aktiv organisasjon



Hva er ekte og hva er falskt?

The image displays two browser windows with their respective certificate details windows open. The top window shows the website <https://norsis.net>. The bottom window shows <https://norsis.no>. Both windows feature a background image of three people in an office setting.

Top Certificate (norsis.net):

Field	Value
Enhanced Key Usage	Server Authenticatio...
Certificate Policies	[1]Certificate Policy:...
CRL Distribution P...	[1]CRL Distribution ...
Authority Informa...	[1]Authority Info Ac...
SCT List	v1, bbd9dfbc1f8a71...
Key Usage	Digital Signature, Ke...
Subject Alternativ...	DNS Name=norsis....
Thumbprint	5f3633a678789c92...

DNS Name=norsis.net
DNS Name=www.norsis.net

Bottom Certificate (norsis.no):

Field	Value
Public key param...	05 00
Enhanced Key Usage	Server Authenticatio...
Subject Key Identi...	be8f20f8dc7c7b425...
Authority Key Ide...	KeyID=a84a6a6304...
Authority Informa...	[1]Authority Info Ac...
Subject Alternativ...	DNS Name=idtyveri...
Certificate Policies	[1]Certificate Policy:...
SCT List	v1, 5581d4c216903...
Key Usage	Digital Signature, Ke...

DNS Name=idtyveri.info
DNS Name=norsis.a2n.no
DNS Name=norsis.no
DNS Name=sikkert.no
DNS Name=www.idtyveri.info
DNS Name=www.norsis.a2n.no
DNS Name=www.norsis.no
DNS Name=www.sikkert.no

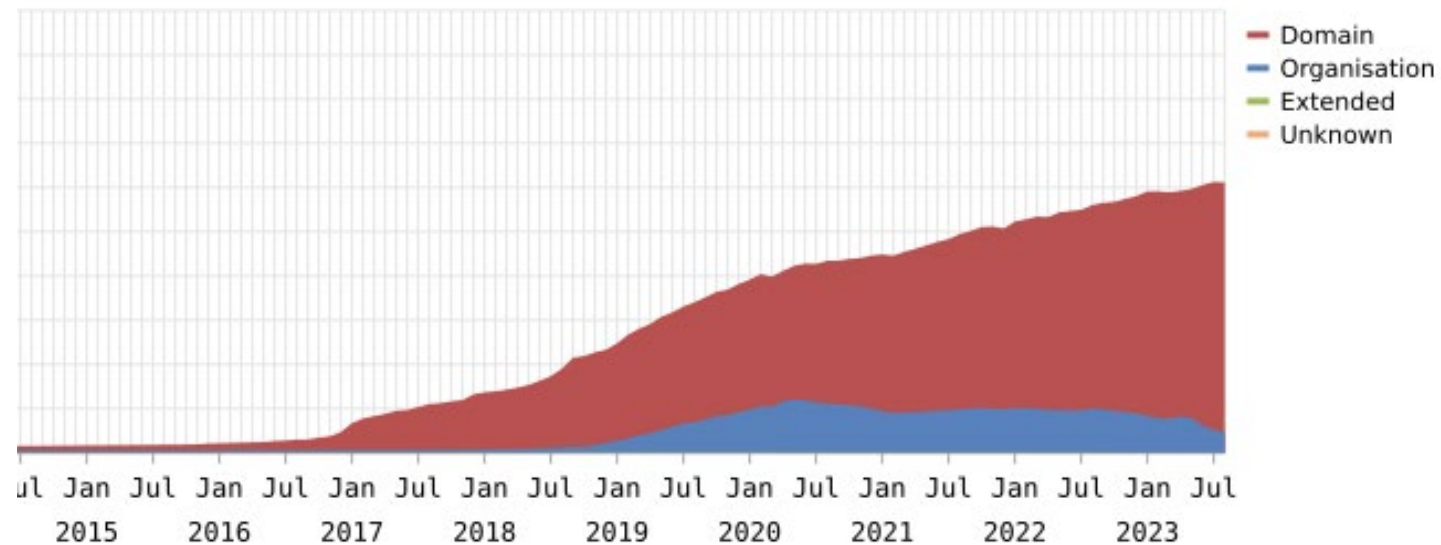
security divas logo and Nasjonal sikkerhetsmåned logo are visible at the bottom of the browser window.

Phishing skjer ved bruk av DV

- Det er enkelt å etablere et falsk domene som kan brukes for svindel ved at dette “likner på” det ekte domenet
- Bruk av EV (med identitet) krever et mer omfattende gjennomført angrep siden mer “falsk” informasjon må etableres i ulike registre
- **Nettleserne er ikke enige**
 - “DV foretrekkes av svindlere fordi de er billige/gratis”
 - “EV gir ingen ekstra sikkerhet, dette forutsetter at sluttbrukerne forstår forskjellen på EV- og DV-sikrede nettsider”
 - “Sluttbrukere må forstå at dine sider er sikret med EV (med identitet) og se etter dette”
- **Nettleserne argumenterer for at sluttbrukere ikke bryr seg**

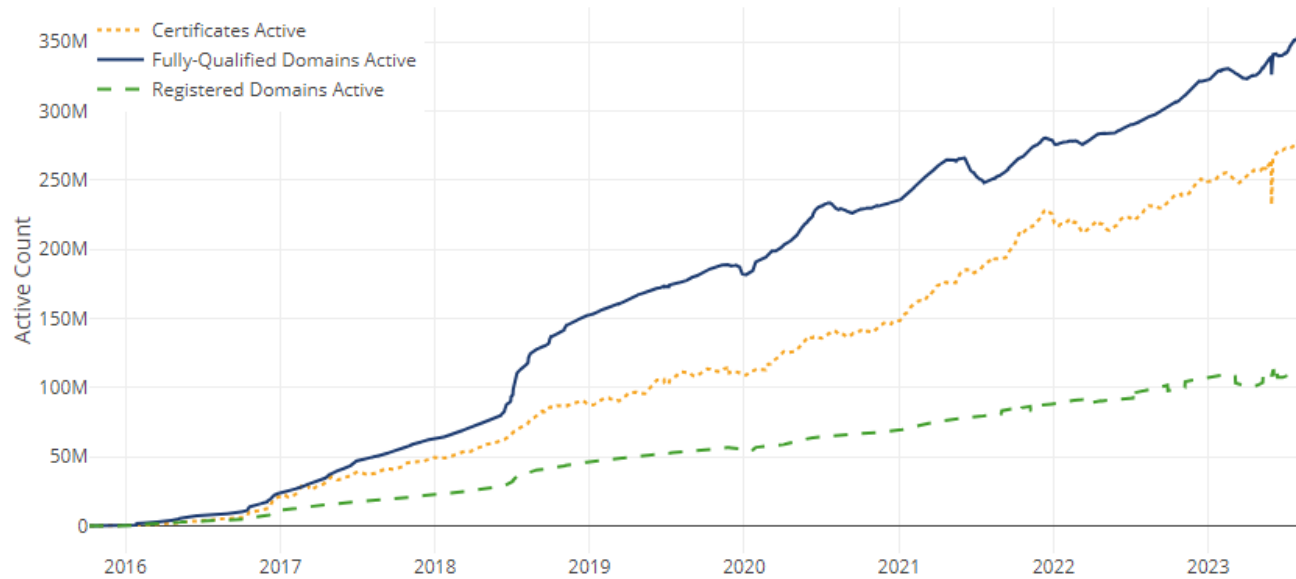
Fordeling på ulike typer sertifikater

Assurance	Current %
Domain	92.59
Organisation	7.31
Extended	0.10
Unknown	0.00
Total Certificates	

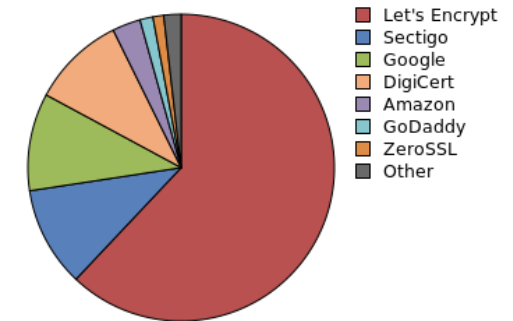


Let's Encrypt – gratis DV-sertifikat

Let's Encrypt Growth



CA Group Market Share



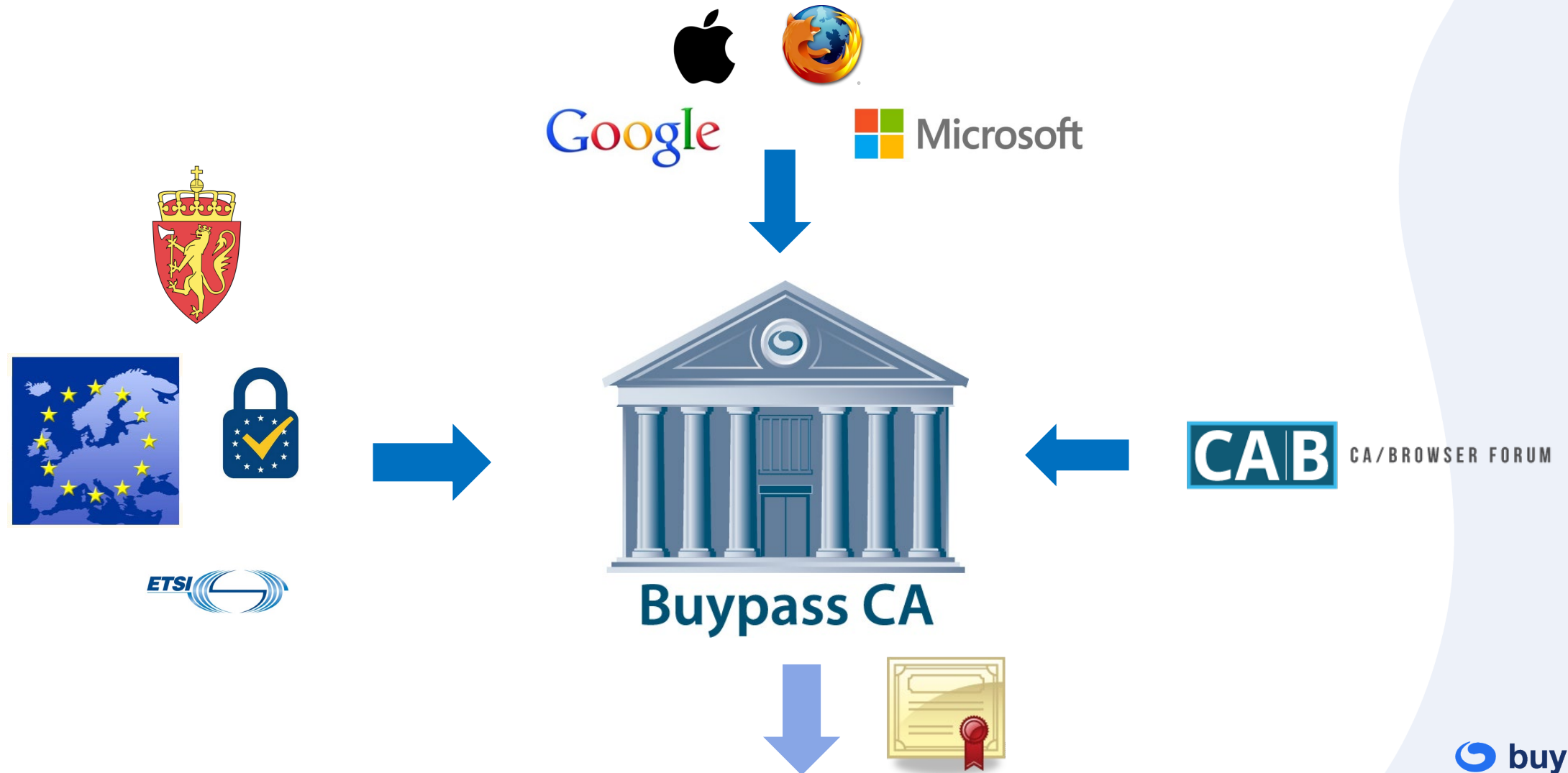
 netcraft

To enable HTTPS on your website, you need to get a certificate (a type of file) from a Certificate Authority (CA). Let's Encrypt is a CA. In order to get a certificate for your website's domain from Let's Encrypt, you have to demonstrate control over the domain. With Let's Encrypt, you do this using software that uses the [ACME protocol](#) which typically runs on your web host.

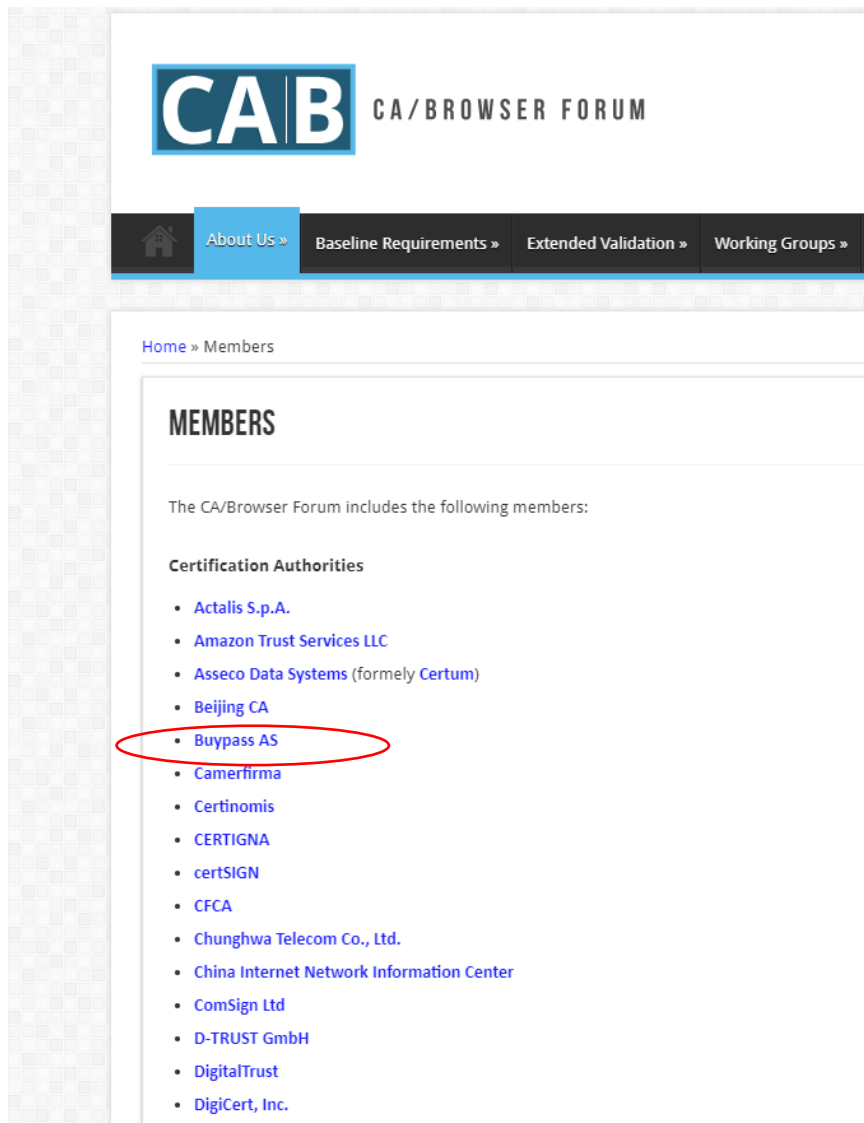
Litt historikk om identitet

Med perspektivet fra Buypass som en CA-operatør

Buypass som CA-operator



CA/Browser Forum



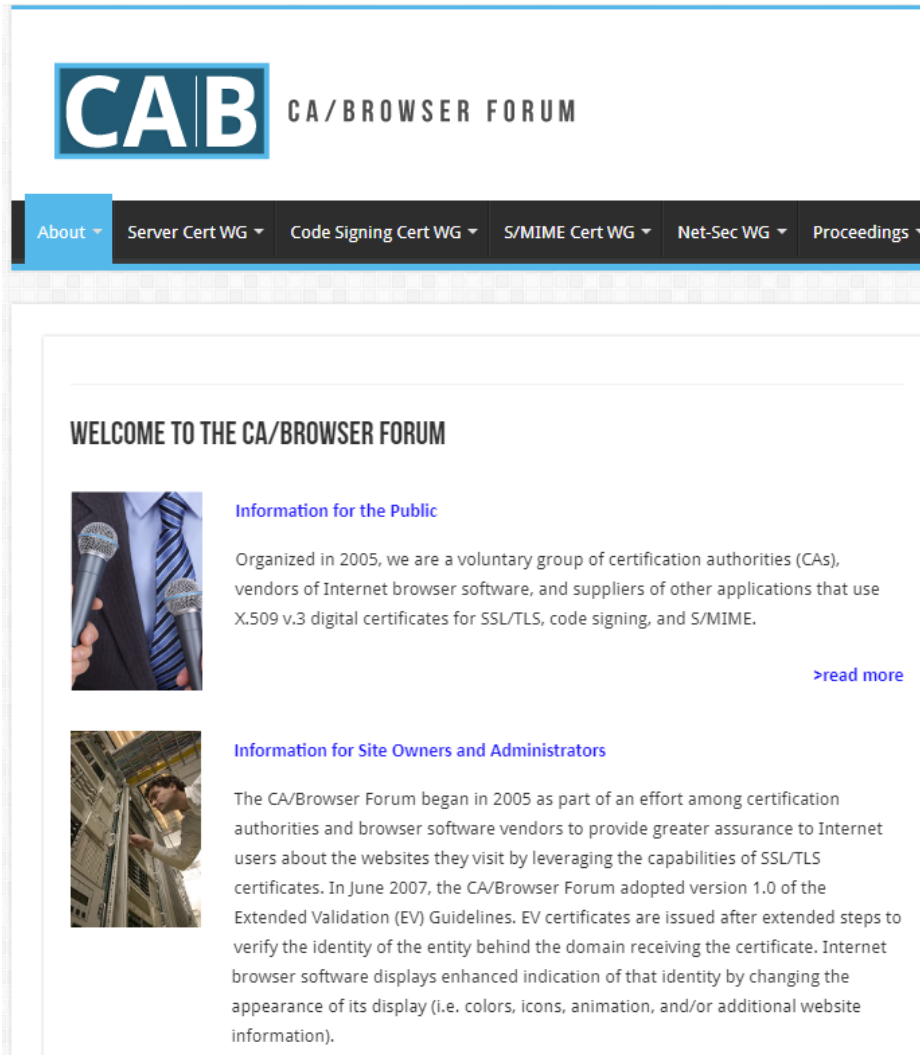
The screenshot shows the CA/Browser Forum website. The header includes the logo and navigation links: Home, About Us, Baseline Requirements, Extended Validation, and Working Groups. The main content area is titled 'MEMBERS' and lists the following members under 'Certification Authorities':

- Actalis S.p.A.
- Amazon Trust Services LLC
- Asseco Data Systems (formerly Certum)
- Beijing CA
- Buypass AS
- Camerfirma
- Certinomis
- CERTIGNA
- certSIGN
- CFCA
- Chunghwa Telecom Co., Ltd.
- China Internet Network Information Center
- ComSign Ltd
- D-TRUST GmbH
- DigitalTrust
- DigiCert, Inc.

The 'Buypass AS' entry is circled in red in the original image.

- En frivillig organisasjon som består av ledende sertifikatutstedere og nettleserleverandører
- Utvikler standarder for utstedelse og administrasjon av digitale sertifikater
 - TLS, CodeSign, S/MIME
- Deltakere pr. 2023 inkluderer Microsoft, Mozilla, Google, Apple, Amazon, Buypass, Sectico, DigiCert, GlobalSign, GoDaddy, Let's Encrypt etc
- cabforum.org

CA/Browser Forum - bakgrunn



The screenshot shows the CA/Browser Forum website. At the top left is the logo 'CAB' in a blue box, followed by 'CA/BROWSER FORUM'. Below the logo is a navigation bar with links: 'About', 'Server Cert WG', 'Code Signing Cert WG', 'S/MIME Cert WG', 'Net-Sec WG', and 'Proceedings'. The main content area has a heading 'WELCOME TO THE CA/BROWSER FORUM'. There are two main sections: 'Information for the Public' and 'Information for Site Owners and Administrators'. The 'Information for the Public' section includes a photo of a person speaking into a microphone and text explaining the forum's purpose. The 'Information for Site Owners and Administrators' section includes a photo of a person working on server racks and text detailing the forum's history and the adoption of EV guidelines in 2007.

WELCOME TO THE CA/BROWSER FORUM

Information for the Public

Organized in 2005, we are a voluntary group of certification authorities (CAs), vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS, code signing, and S/MIME.

[>read more](#)

Information for Site Owners and Administrators

The CA/Browser Forum began in 2005 as part of an effort among certification authorities and browser software vendors to provide greater assurance to Internet users about the websites they visit by leveraging the capabilities of SSL/TLS certificates. In June 2007, the CA/Browser Forum adopted version 1.0 of the Extended Validation (EV) Guidelines. EV certificates are issued after extended steps to verify the identity of the entity behind the domain receiving the certificate. Internet browser software displays enhanced indication of that identity by changing the appearance of its display (i.e. colors, icons, animation, and/or additional website information).

- Etablert i 2005
- Første standard i 2007 for utstedelse av Extended Validation (EV) sertifikater
 - Identitet var en viktig faktor sammen med omfattende kontroller for å gjøre det trygt på nett i en verden der det ellers var “vill-vest” tilstander
- Baseline Requirements i 2012
 - Minimumsnivå for alle typer TLS sertifikater
- Buypass med fra 2008

Identitet i TLS-sertifikater – EV i går



The screenshot shows the BuyPass website interface. At the top, the browser address bar is highlighted with a red box, displaying the URL <https://www.bypass.no/produkter-c>. The website header includes the BuyPass logo with the tagline "securing transactions", navigation links for "Logg inn", "English", "AAA", a shopping cart, and a search bar. Below the header, there are three main menu items: "PRODUKTER & TJENESTER", "BRANSJER", and "BRUKER". The main content area features a grid of logos for various clients, including Lånekassen, eika., SLENGAER KOMMUNE, NSM, POLITIET, FAUSKE KOMMUNE, Nemko, NORSK TIPPING, BKK, Laerdal, DSS, Akershus universitetssykehus, Stryn kommune, EVRY, Gjensidige, BLUEGARDEN, BERUM KOMMUNE, Hurdal Kommune, and Helsedirektoratet. To the right of the logos, the text reads "Tar trygghet på alvor" followed by "Domene, Business og EV-sertifikater. Levert som enkelt sertifikat, wildcard og multidomener." Below the client logos, there is a navigation bar with buttons for "SSL-sertifikater", "SSL Domain", "SSL Business", "SSL EV", "Sammenlign", and "Priser".

SSL-sertifikater



Identitet i TLS-sertifikater – EV i dag

buypass.no

buypass Bedrift Person Om

BUYPASS AS
Trygg digitalt

buypass.no

- Connection is secure
- Cookies and site data
- Site settings
- About this page

Security buypass.no

- Connection is secure
- Certificate is valid
Issued to: BUYPASS AS [NO]

Certificate Viewer: www.buypass.no

General Details

Issued To

- Common Name (CN) www.buypass.no
- Organization (O) BUYPASS AS
- Organizational Unit (OU) <Not Part Of Certificate>

Issued By

- Common Name (CN) Buypass Class 3 CA 2
- Organization (O) Buypass AS-983163327
- Organizational Unit (OU) <Not Part Of Certificate>

Validity Period

- Issued On Thursday, February 2, 2023 at 4:54:16 PM
- Expires On Sunday, February 18, 2024 at 11:59:00 PM

Fingerprints

- SHA-256 Fingerprint CE B1 89 04 D1 D3 B0 E8 84 C3 98 96 70 3D 1C CD 74 2E A8 A2 DC 21 08 B8 E7 FF F4 67 FE 7C 74 FB
- SHA-1 Fingerprint AF BF A2 9D 95 76 7C 02 AD 1A E9 65 B3 7A F9 59 99 16 1B 1E

sikkerhetsfestivalen.no

- Connection is secure
- Certificate is valid

Certificate Viewer: sikkerhetsfestivalen.no

General Details

Issued To

- Common Name (CN) sikkerhetsfestivalen.no
- Organization (O) <Not Part Of Certificate>
- Organizational Unit (OU) <Not Part Of Certificate>

Issued By

- Common Name (CN) R3
- Organization (O) Let's Encrypt
- Organizational Unit (OU) <Not Part Of Certificate>

Validity Period

- Issued On Thursday, August 10, 2023 at 10:08:45 PM
- Expires On Wednesday, November 8, 2023 at 9:08:44 PM

Fingerprints

- SHA-256 Fingerprint 07 18 DA 38 DB 6C CC 74 B2 C6 80 9F 55 0F BE 48 37 37 E6 2D C6 BC 9F FC 73 AC D6 17 43 0C 7E DD
- SHA-1 Fingerprint D5 69 99 FA 99 1C 64 06 16 78 2D 7D 1D 88 87 76 11 D3 4F 2E

Argumentasjonen mot EV fra nettlesere

The server's identity

I've said that the certificate contains the server's identity, but not what that identity consists of. The most common scenario is that certificate just contains the **domain name** of the server. So, the certificate for `https://educatedguesswork.org` would contain the name `educatedguesswork.org`. When the browser connects to the site, it verifies that the domain name in the certificate matches the domain name it is trying to connect to. In practice, certificates often contain other information, such as the organization to which it was issued, but **the browser does not use it to establish the connection.**

As an example, here's the "subject" information from Twitter's certificate:

Field	Value
Common Name	<code>twitter.com</code>
Organization	Twitter, Inc.
Location	San Francisco
State	California
Country	US

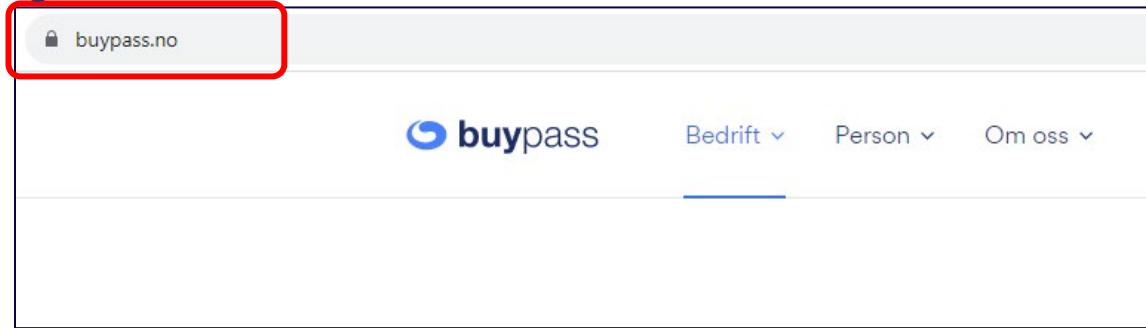
<https://educatedguesswork.org/posts/eidas-article45/>

EV certificates were one of those plausible ideas that were worth a try but turn out not to work, for two distinct reasons.

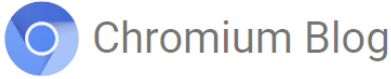
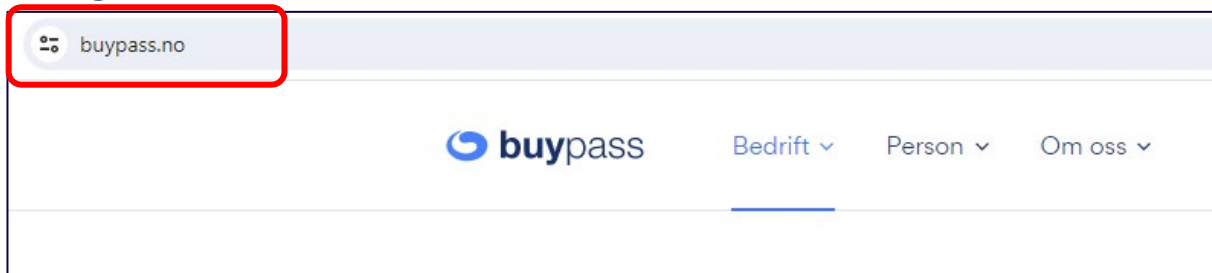
- **Users Don't Check.** The basic premise of EV is that users will look at the UI and behave differently when the EV indicator (the company name) is displayed. Unfortunately, this seems not to be the case. Chrome's Security team does a good job of **summarizing the research** in this area, but the TL;DR is that if you remove the EV indicator for sites, most people don't seem to notice or behave differently.
- **Names Aren't Unique.** Organizational names are generally scoped by jurisdiction, which allows an attacker to register a company with the same name as the company they are impersonating and then get an EV certificate. In one famous **incident**, security researcher Ian Carroll got an EV certificate for "Stripe Inc." by registering a legal entity in a different state and then applying for an EV cert.

HTTPS i dag og i morgen (Chrome)

I dag:



I morgen:

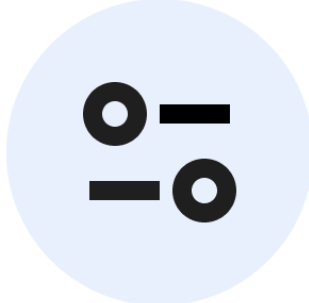


Chromium Blog
News and developments from the open source browser project

An Update on the Lock Icon

Tuesday, May 2, 2023

Editor's note: based on industry research (from Chrome and others), and the ubiquity of HTTPS, we will be replacing the lock icon in Chrome's address bar with a new "tune" icon – both to emphasize that security should be the default state, and to make site settings more accessible. Read on to learn about this multi-year journey.



We plan to replace the lock icon with a variant of the tune icon, which is commonly used to indicate controls and settings.

Replacing the lock icon with a neutral indicator prevents the misunderstanding that the lock icon is associated with the trustworthiness of a page, and emphasizes that security should be the default state in Chrome. Our research has also shown that many users never understood that clicking the lock icon showed important information and controls. We think the new icon helps make permission controls and additional security information more accessible, while avoiding the misunderstandings that plague the lock icon.

eIDAS 2.0

QWAC: Qualified Website Authentication Certificate

eIDAS-forordningen

Regulation (EU) No 910/2014 of 23 July 2014

Electronic identification (eID) and Trust Services for my business

eIDAS SOLUTIONS

for electronic
and re

The screenshot shows the LOVDATA website interface. At the top, there is a search bar with the text "Søk etter lover, forskrifter, dommer og stortingsvedtak". Below the search bar, the main content area displays the title of the regulation: "Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektr...". A button labeled "Gå til opprinnelig kunnngjort versjon" is visible. The regulation details are presented in a table:

Dato	LOV-2018-06-15-44
Departement	Nærings- og fiskeridepartementet
Ikrafttredelse	15.06.2018
Endrer	LOV-2001-06-15-81
Kunngjort	15.06.2018
Korttittel	Lov om elektroniske tillitstjenester

Below the table, the text reads: "Jf. tidligere lov 15. juni 2001 nr. 81. – Jf. EØS-avtalen vedlegg XI nr. 5I (forordning (EU) nr. 910/2014)."

§ 1. eID og elektroniske tillitstjenester i EØS



The eSeal logo is shown with the text "eSeal guarantee both the origin and the integrity of a document." Below it, three benefits are listed in purple boxes: "HELPS AVOID FISHING, PROTECTING THE REPUTATION OF YOUR BUSINESS", "REDUCED COSTS AND TIME THROUGH STREAMLINED PROCESSES", and "TRUST IN THE ORIGIN OF THE DOCUMENT". To the right, a blue box says "ENHANCED DOCUMENT TRACKING".

Buypass som tilbyder av tillitstjenester



The screenshot shows the EU Trust Services Dashboard for Buypass AS. At the top, there is the European Commission logo and the text "EU Trust Services Dashboard". Below this is a navigation bar with a home icon, "DISCOVER", "BROWSE", and "TRY". The breadcrumb trail reads "CEF eSignature / EU Trust Services Dashboard / Browse / Trusted Lists / Norway / Trust service provider". The main content area features the Buypass AS logo (a red and white flag) and the text "Trust services". Below this are three service cards: "QCert for ESig" (Qualified certificate for electronic signature), "QCert for ESeal" (Qualified certificate for electronic seal), and "QWAC" (Qualified certificate for website authentication). At the bottom, there is a "Detailed information" link.

QWAC – et kvalifisert TLS-sertifikat

Electronic identification (eID) and Trust Services for my business

eIDAS SOLUTIONS

Take advantage of cross-border business opportunities
Increase efficiency & security of your business + Improve user experience

The infographic features a central gear with a map of Europe, surrounded by icons for different services: eSignature, eTimestamp, eID, eSeal, and Qualified Web Authentication Certificate (QWAC). Each service is accompanied by a brief description and a list of benefits. The QWAC section is highlighted with a red border.

eSignature
expression in an electronic format of a person's agreement to the content of a document.

- REDUCED COSTS AND TIME THROUGH STREAMLINED PROCESSES
- MORE INNOVATIVE BUSINESS PROCESSES
- CONVENIENCE FOR BUSINESS AND CUSTOMER

eTimestamp
electronic proof that a set of data existed at a specific time.

- ENHANCED DOCUMENT TRACKING
- GREATER ACCOUNTABILITY

eID
A way for businesses and consumers to prove their identity electronically.

- EXPANSION OF CUSTOMER BASE
- COST AND TIME SAVING
- TRUST IN CROSS-BORDER TRANSACTIONS
- CONVENIENCE FOR BUSINESS AND CUSTOMER

eSeal
guarantee both the origin and the integrity of a document.

- REDUCED COSTS AND TIME THROUGH STREAMLINED PROCESSES
- TRUST IN THE ORIGIN OF THE DOCUMENT

Qualified Web Authentication Certificate (QWAC)
ensure your website is trustworthy and reliable.

- INCREASED CONSUMER TRUST
- HELPS AVOID FISHING, PROTECTING THE REPUTATION OF YOUR BUSINESS

Electronic Registered Delivery Service
protects against the risk of loss, theft, damage or alterations when sending documentation

- REDUCED TIME AND COSTS IN DOCUMENT EXCHANGE
- INCREASED EFFICIENCY AND TRUST
- ENHANCED DOCUMENT TRACKING

- QWAC er et kvalifisert sertifikat under eIDAS-forordningen
- Dette er basert på kravene til EV-sertifikater med sterk fokus på identitet
- Med i eIDAS siden 2016

Lovforslag 3.juni 2021 => eIDAS 2.0



Brussels, 3.6.2021
COM(2021) 281 final

2021/0136 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

- Oppdatering av eIDAS
- Fokus på identitetsrammeverk og digital lommebok
- Men også enkelte andre viktige endringer
 - QWAC i artikkel 45

Endringer vedr QWAC

SECTION 8

Website authentication

Article 45

Requirements for qualified certificates for website authentication

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV.
2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the requirements laid down in website authentication meets those standards. Those implementing procedure referred to in Article 48(2).

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. Qualified certificates for website authentication shall be deemed compliant with the requirements laid down in Annex IV where they meet the standards referred to in paragraph 3.
2. Qualified certificates for website authentication referred to in paragraph 1 shall be recognised by web-browsers. For those purposes web-browsers shall ensure that the identity data provided using any of the methods is displayed in a user friendly manner. Web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1, with the exception of enterprises, considered to be microenterprises and small enterprises in accordance with Commission Recommendation 2003/361/EC in the first 5 years of operating as providers of web-browsing services.
3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, provide the specifications and reference numbers of standards for qualified certificates for website authentication referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

Hvorfor gjør EU dette?

- **Skape trygghet hos innbyggere i EU som benytter tjenester på nett**
 - De har rett til å vite hvem de samhandler med
- **Det bør være opp til europeiske myndigheter og deres suverenitet å bestemme dette**
 - For viktig til å overlates til store selskaper (“big tech”) som opererer under en helt annen lovgivning enn EUs
- **EU har lenge forsøkt å få nettlekere til å samarbeide om dette, men dette har feilet**
 - Nettlekerne har tvertimot gått i en helt annen retning og gjort tilgang på identitetsinformasjon mindre tilgjengelig for sluttbrukere de seneste årene

Forslaget møter motstand

Mozilla Campaign: securityriskahead.eu



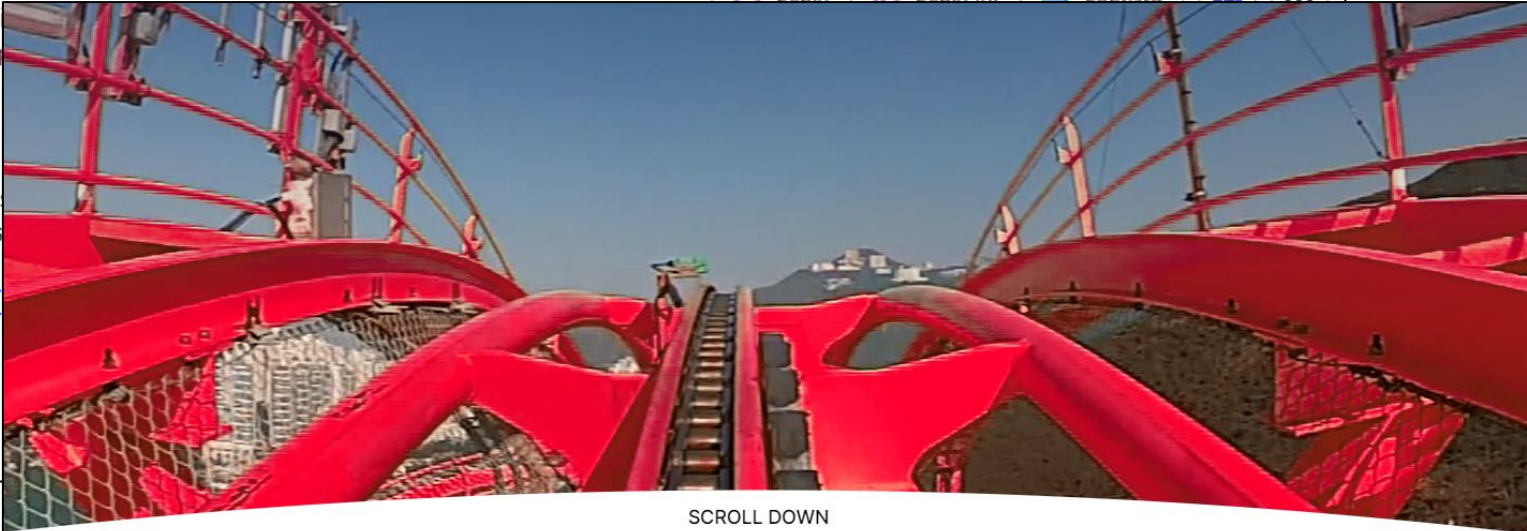
dev-security-pol
To dev-security-

All,

This is just FYI that Mozilla has
(written) could force browsers

<https://securityriskahead.eu/>

Cheers,
Kathleen



SCROLL DOWN



WHY ARE QWACs A PROBLEM?

When using the internet, your browser protects valuable information you send to websites. But eIDAS article 45.2 will force browsers to accept QWACs – lower-security standard website certificates and providers that issue them. By complying, browsers would open users up to possible malicious attacks and online crime.

In short, eIDAS article 45.2 will lower the bar for protection. And those few sentences make the internet less safe.

Hvorfor er nettleserne negative?

- Nettleserne sier at QWACs har en lavere sikkerhetsstandard enn de sertifikatene de selv aksepterer via egne rotsertifikatprogram
- Nettleserne er skeptiske til å akseptere sertifikatutstedere (QTSP-er) som ikke er vurdert opp mot rotsertifikatprogrammernes egne sikkerhetskrav
 - eIDAS har et styringsregime som nettleserne ikke stoler fullt og helt på
- Nettleserne er mest opptatt av HTTPS-kryptering og ikke interessert i å bruke ressurser på identitet (de mener at “EV har feilet”)
- Nettleserne mener at dette kan gi insentiver for myndigheter i andre mindre innbyggervennlige land å lage egne reguleringer for å overvåke sine innbyggere

Article 45.2 requires browsers to accept and display Qualified Website Authentication Certificates.



Men argumentene møter motstand



Mozilla website pushes serious eIDAS misinformation to political decision makers and public

The discussion on the eIDAS Regulation has entered its most important phase in the European Parliament and Council. Mozilla has recently [launched a campaign](#) in the form of a website aimed at political decision-makers, but also the general public.

The campaign pushes **serious misinformation** on the eIDAS legislation in order to block changes to Article 45 covering the EU's Qualified Web Authentication Certificates ("QWACs). These certificates are used to secure AND identify websites for the highest level of EU consumer protection.

Mozilla's goal is to frighten Parliament and Council members that the European Union's eIDAS law is bad for user security. That's FALSE. Instead, the legislation will **increase the online security of European citizens**.

This is just another example of US big tech companies trying to control all decisions about security to favor their own commercial interests.

MOZILLA SAYS:

"A new EU law would make website security weaker by imposing QWACs and expose users to more cyber risks. eIDAS article 45.2 will force browsers to accept QWACs — lower-security standard website certificates and providers that issue them."

1

QWACs are just like all the every other webserver certificate that Mozilla already trusts — so QWACs are **not** in any way "lower-security" website certificates.

THE FACTS:

THESE STATEMENTS ARE FALSE

MOZILLA SAYS:

*"When you see the **padlock** on the left side of the URL bar in the browser, you know your connection with the website is **fully secure**."*

2

Mozilla likes to use the word "secure", when all Mozilla is saying is that communications between a website and a user are **encrypted** (so they can't be read by a third party in transit). Encryption is the **bare minimum** for user "security", and QWACs enable encryption, like all other website certificates.

THE FACTS:

VERY MISLEADING

Dialog mellom ETSI og nettlesere

ETSI TR 119 411-5 V1.1.1 (2023-01)



**Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for
Trust Service Providers issuing certificates;
Part 5: Guidelines for the coexistence of
web browser and EU trust controls**

Introduction

Transport Layer Security (TLS) [i.7], including earlier versions based on Secure Socket Layer (SSL), is an integral part of the security environment for the web. TLS/SSL is widely supported by web browsers and websites. A TLS connection between a browser and a website depends on a website's authentication certificate, often referred to as a "server certificate" which binds its domain name, and optionally, the genuine and legitimate entity standing behind the website, to a public key.

Browser Vendors operate individual Root Programs to review and approve root certificates linked via a certificate chain to website authentication certificates. Trusted root certificates are included in a Root Store used by the web browser to validate website certificates used in TLS/SSL.

Regulation (EU) No 910/2014 [i.4] is a regulation on electronic identification and trust services for electronic transactions in the internal market. Under Regulation (EU) No 910/2014 [i.4], EU Commission and EU member states operate a trust scheme for the approval of trust services, including issuers of qualified certificates for website authentication. Trusted issuers of website certificates are listed in EU Trusted Lists according to EU Commission Implementing Decision 2015/1505. Further requirements on web browsers for recognition and display of website certificates are under review.

The CA/Browser Forum is an unincorporated association of separate certificate issuers (i.e. EU Qualified Trust Service Providers and Certification Authorities), certificate consumers (e.g. web browsers), and interested parties. Members of the CA/Browser Forum maintain a standard set of minimum requirements and expectations for the issuance of publicly-trusted website certificates. Both Browser Vendor Root Stores, the EU trust scheme, and the ETSI policy and security requirements for QTSPs and QWACs incorporate features of the CA/Browser Forum Requirements [i.6].

So far, browsers were not checking website's certificates against any EU Trusted List. Therefore, the present document provides guidance to perform such a check and enable the coexistence of trust controls applied by the Browser Vendors and EU trust scheme to EU qualified certificates for website authentication.

Status eIDAS 2.0

- **eIDAS 2.0 er nå inne i såkalte trilogiforhandlinger;**
 - Uformelle forhandlinger mellom Kommisjonen, Europaparlamentet og Rådet som skal ende opp med den endelige lovteksten for eIDAS 2.0
- **Forhandlingene pågår og forventes at teksten er klar i løpet av September**
 - Lovteksten for QWACs er omtrent uforandret, men det kommer en åpning for nettleiere kan avvise enkelte QTSP-er/QWAC-er dersom de kan dokumentere at dette skaper problemer for sikkerheten på nett etter deres mening
- **Det skal deretter stemmes og lovteksten vil være vedtatt rundt årsskiftet**

**Vil identitet få sin
renessanse?**

Vil identitet i TLS få sin renessanse?

- eIDAS 2.0 vil med stor sannsynlighet komme med krav til at nettleserne må anerkjenne QWACs og bidra til at sluttbrukere får informasjon om identiteten til aktøren som står bak nettsiden
- Nettleserne er nok fortsatt skeptisk til dette, men EU har flere maktmidler som kan brukes, bla nylig etablerte reguleringer som Digital Markets Act og Digital Services Act
- Bruk av QWACs vil være frivillig, men det er grunn til å tro at offentlige myndigheter i EU vil bli anbefalt å ta i bruk QWACs på sine nettsider for å beskytte sine innbyggere

Spørsmål?

