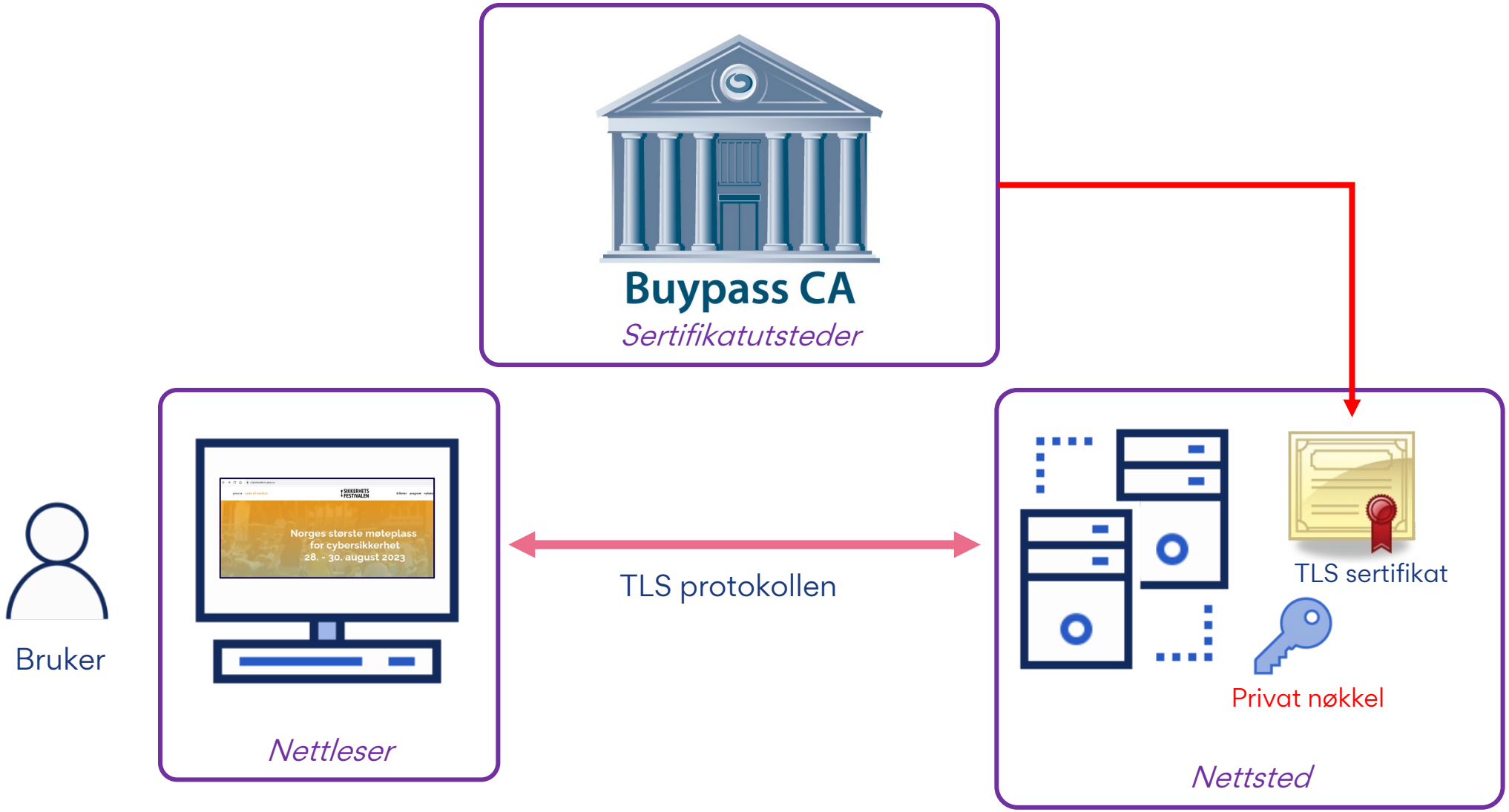
Er identitet i HTTPS/TLS i ferd med å få sin renessanse?

buypass

HTTPS-kryptering på nett

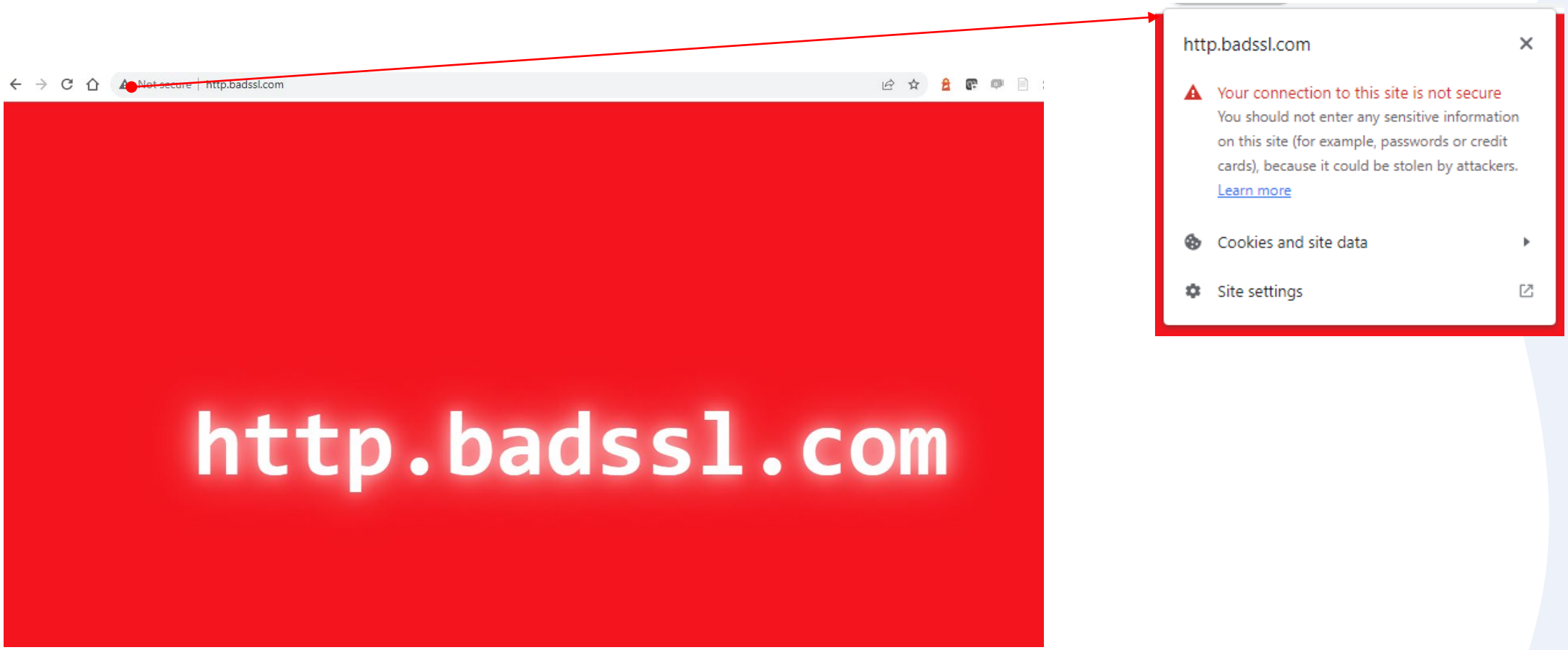
buypass

Økosystemet rundt HTTPS/TLS



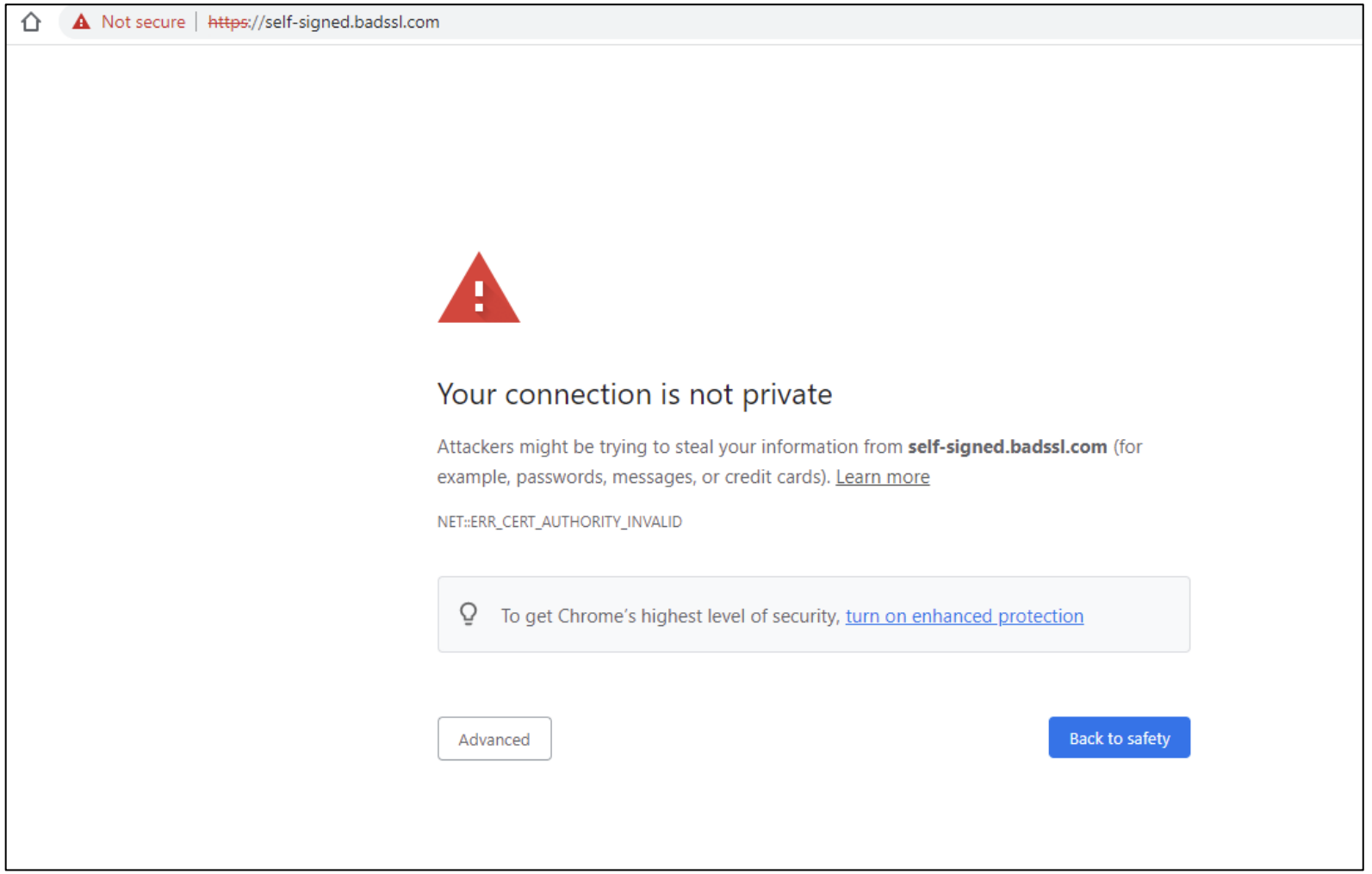
buypass

Hvorfor er HTTPS-kryptering viktig?



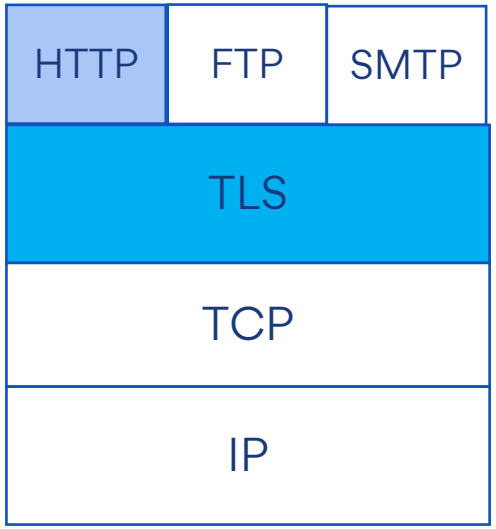
buypass

Nettlesere blokkerer tilgang



buypass

Hva er HTTPS og TLS?



- 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

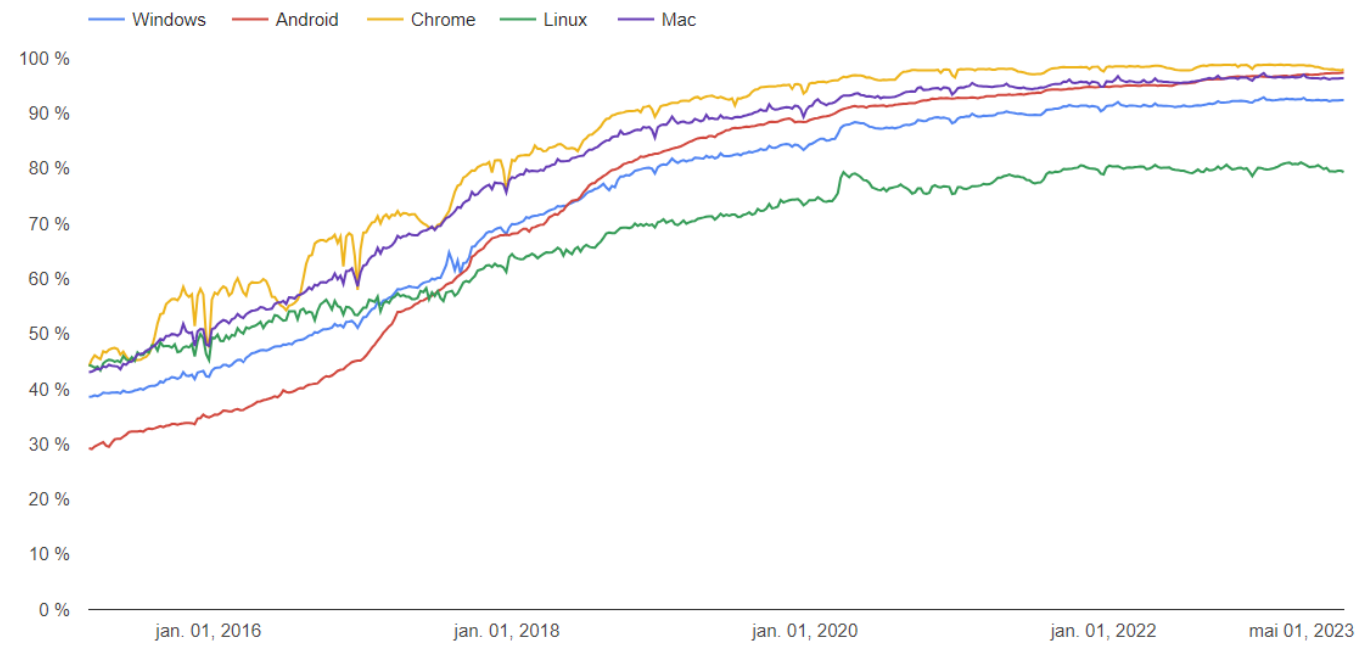
buypass

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



https://transparencyreport.google.com/https/overview

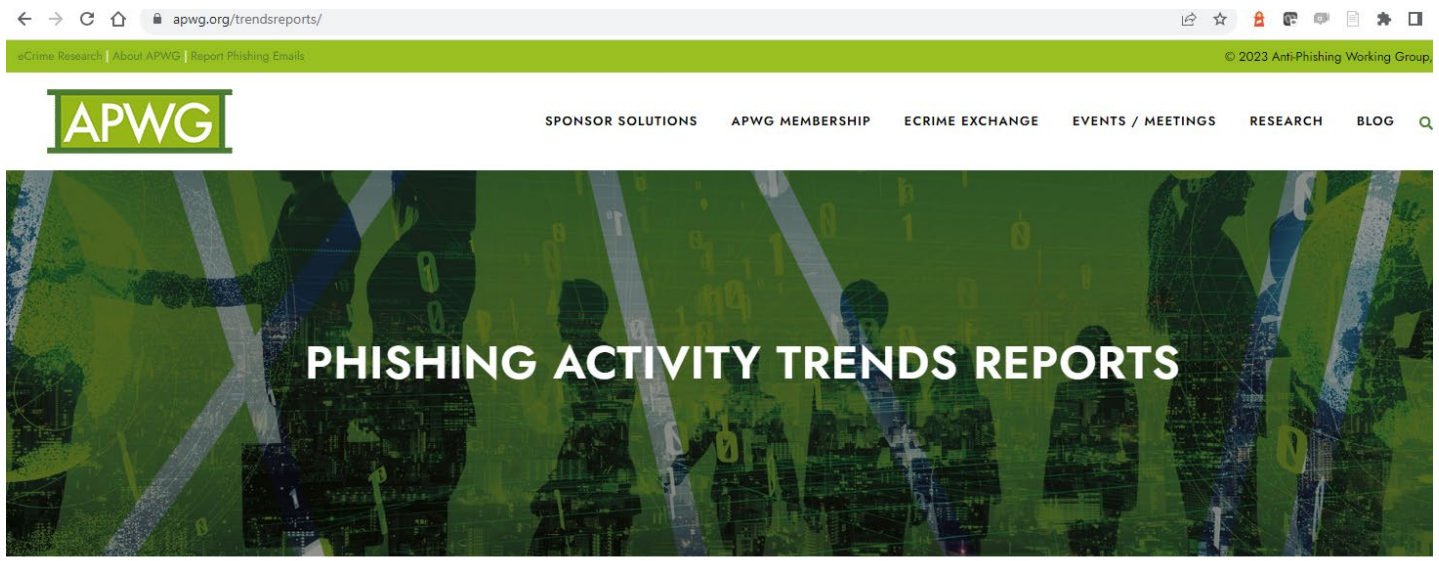
buypass

Phising øker stadig!

På tross av HTTPS-kryptering

buypass

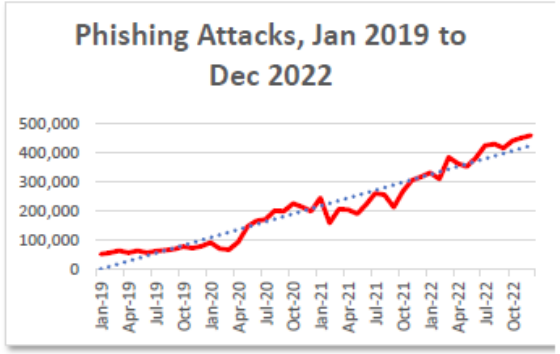
Antall phishing sites øker



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



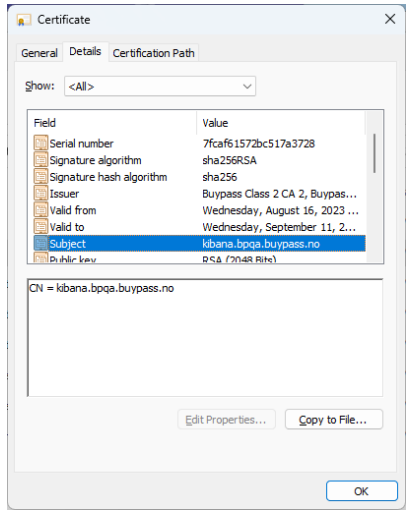
The year 2022 was another record-shattering year for phishing, with the APWG logging more than 4.7 million attacks

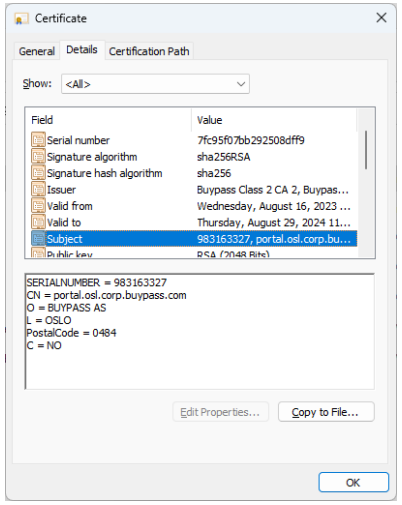
	October	November	December
Number of unique phishing Web sites (attacks) detected	440,508	450,390	459,139
Unique phishing email subjects	101,104	77,469	74,250
Number of brands targeted by phishing campaigns	599	610	577

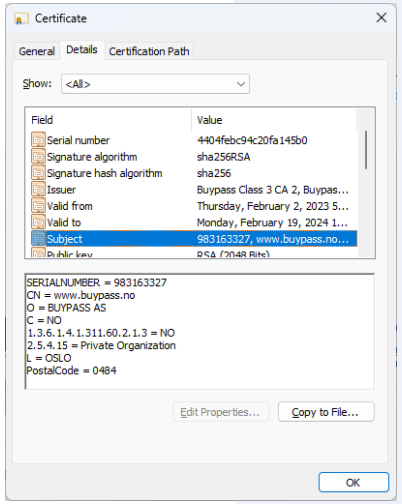
buypass

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

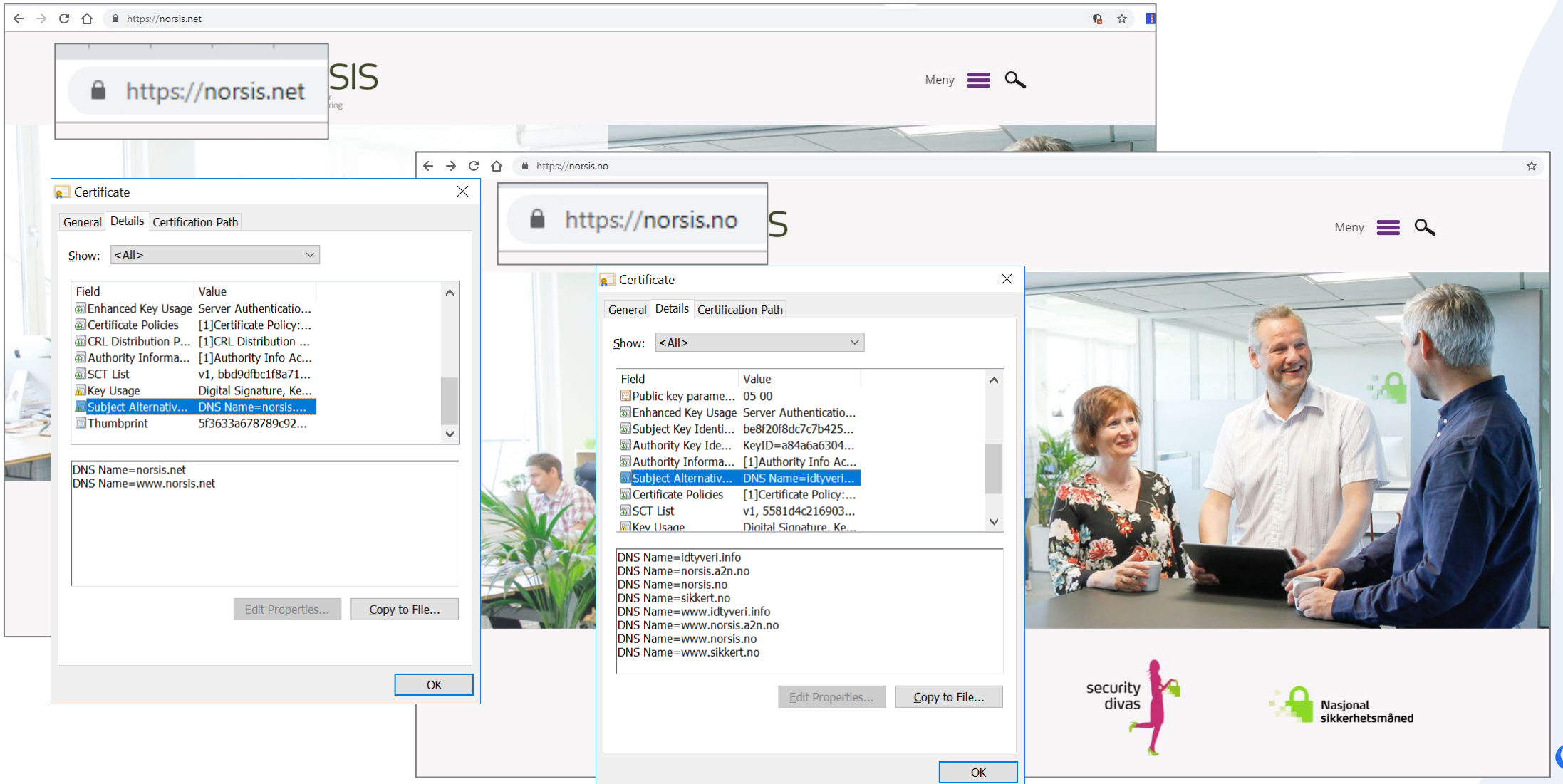






buypass

Hva er ekte og hva er falskt?



buypass

Phishing skjer ved bruk av DV

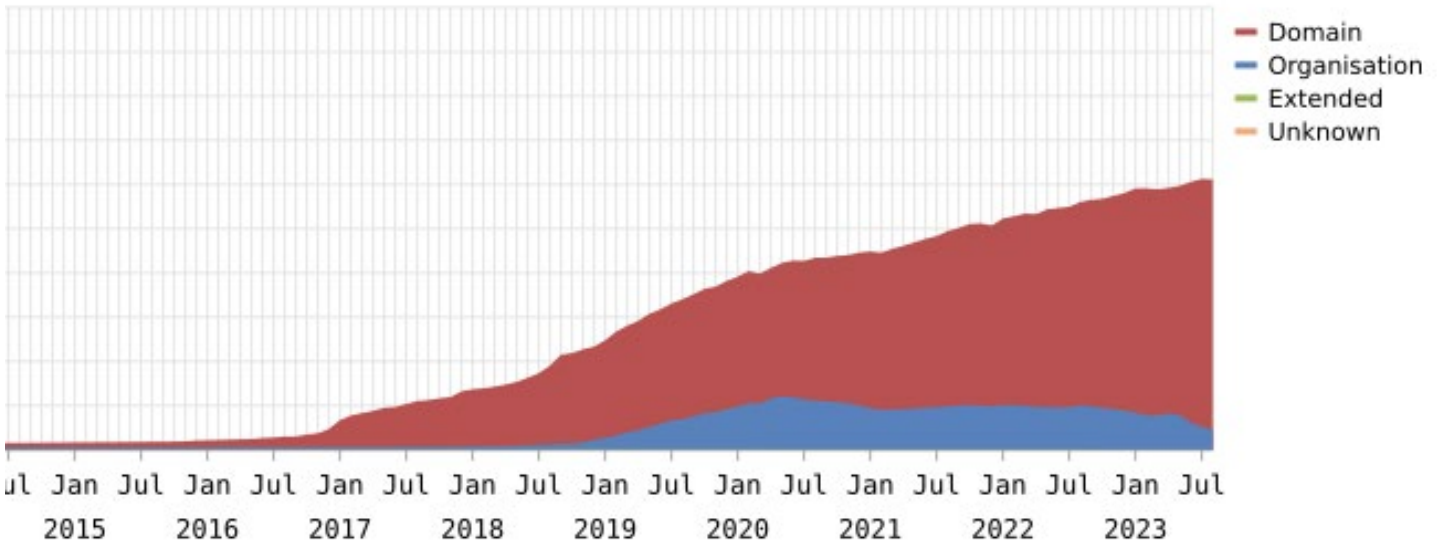
- Det er enkelt å etablere et falsk domene som kan brukes for svindel ved at dette "likner på" det ekte domenet
- Bruk av EV (med identitet) krever et mer omfattende gjennomført angrep siden mer "falsk" informasjon må etableres i ulike registre

- 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

buypass

Fordeling på ulike typer sertifikater

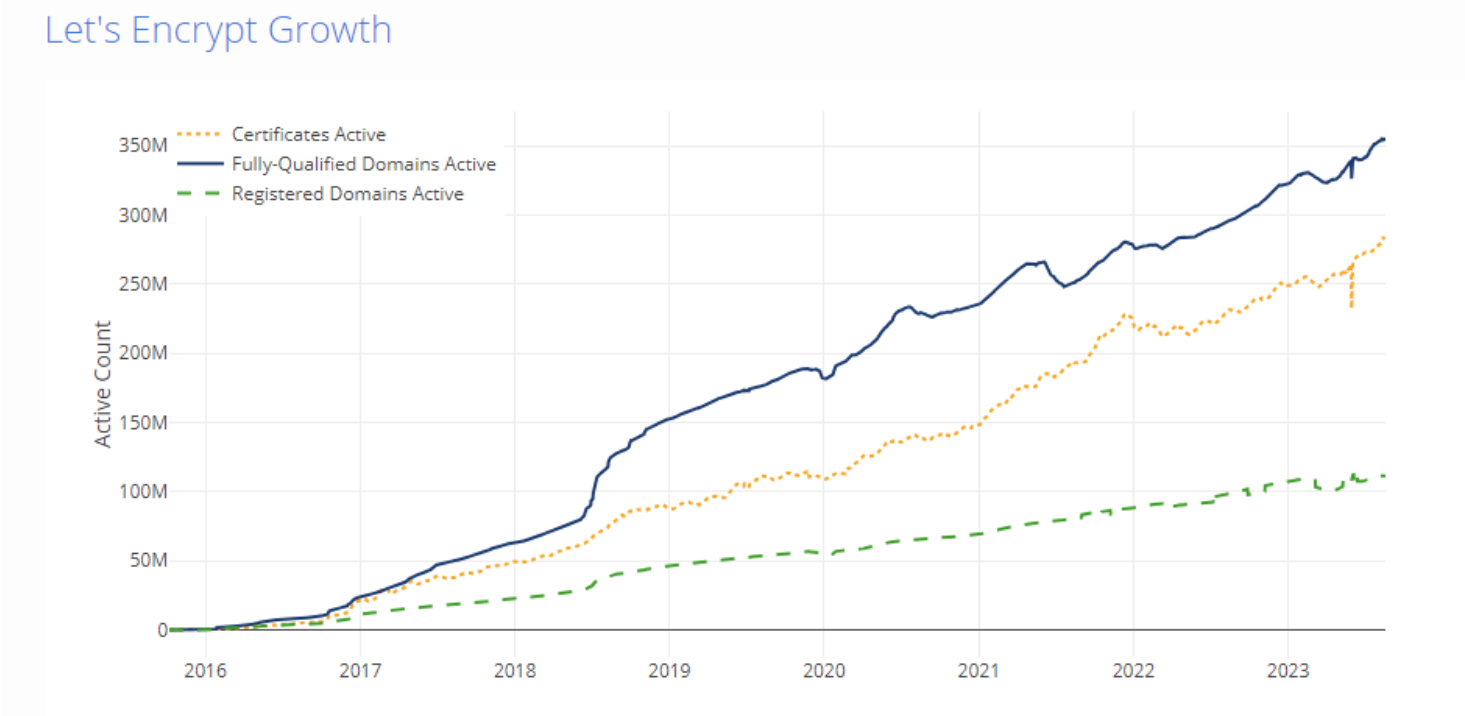
Assurance	Current %
Domain	92.59
Organisation	7.31
Extended	0.10
Unknown	0.00
Total Certificates	

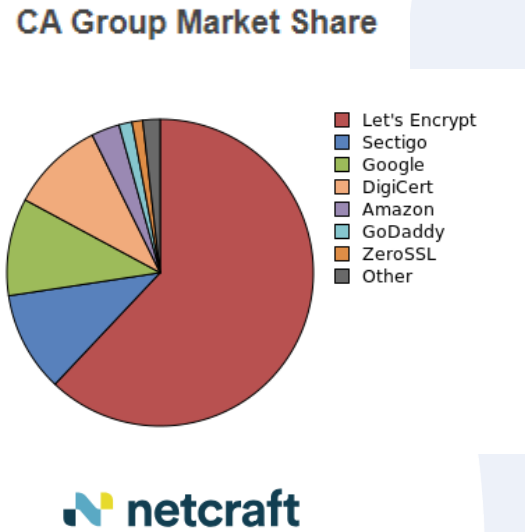


netcraft

buypass

Let’s Encrypt – gratis DV-sertifikat





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.

Let’s Encrypt

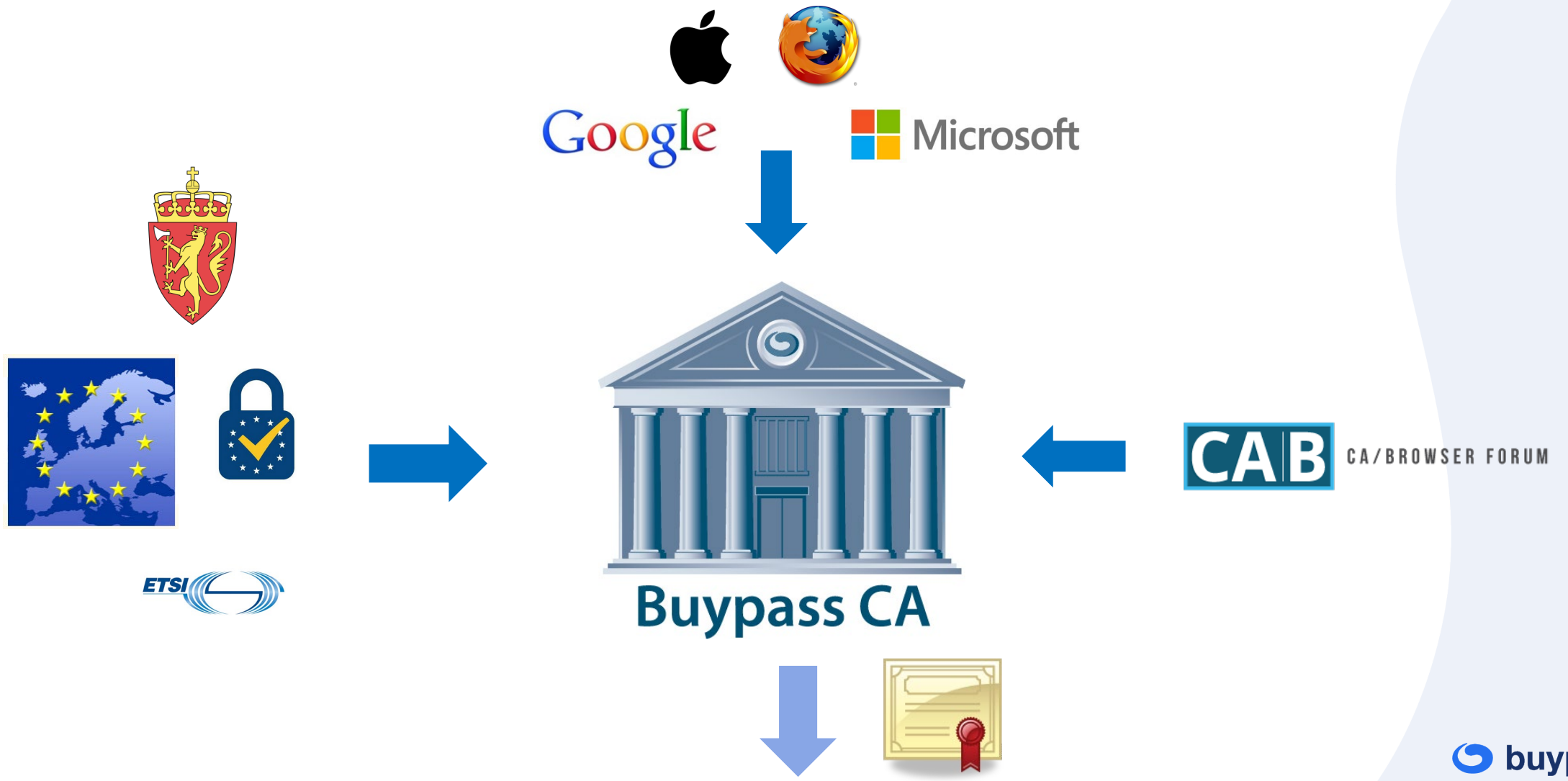
buypass

Litt historikk om identitet

Med perspektivet fra Buypass som en CA-operatør

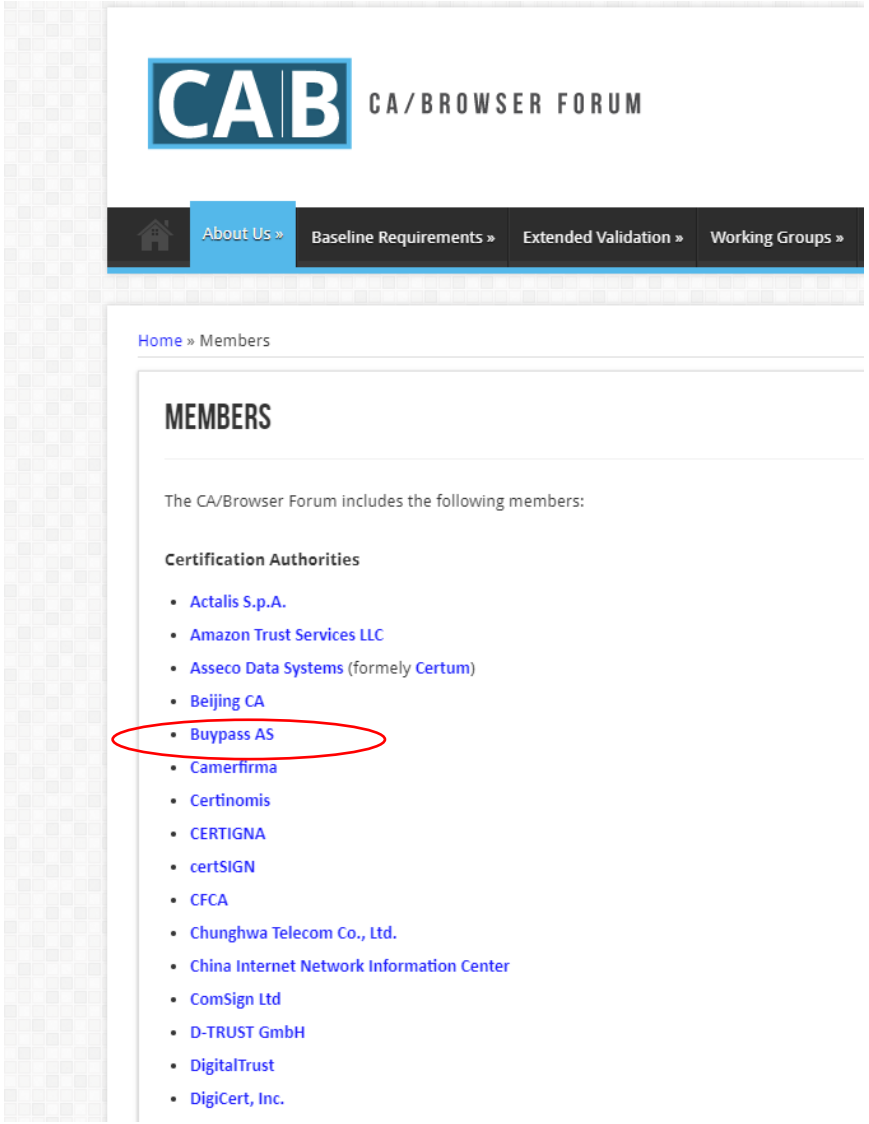
buypass

Buypass som CA-operatør



buypass

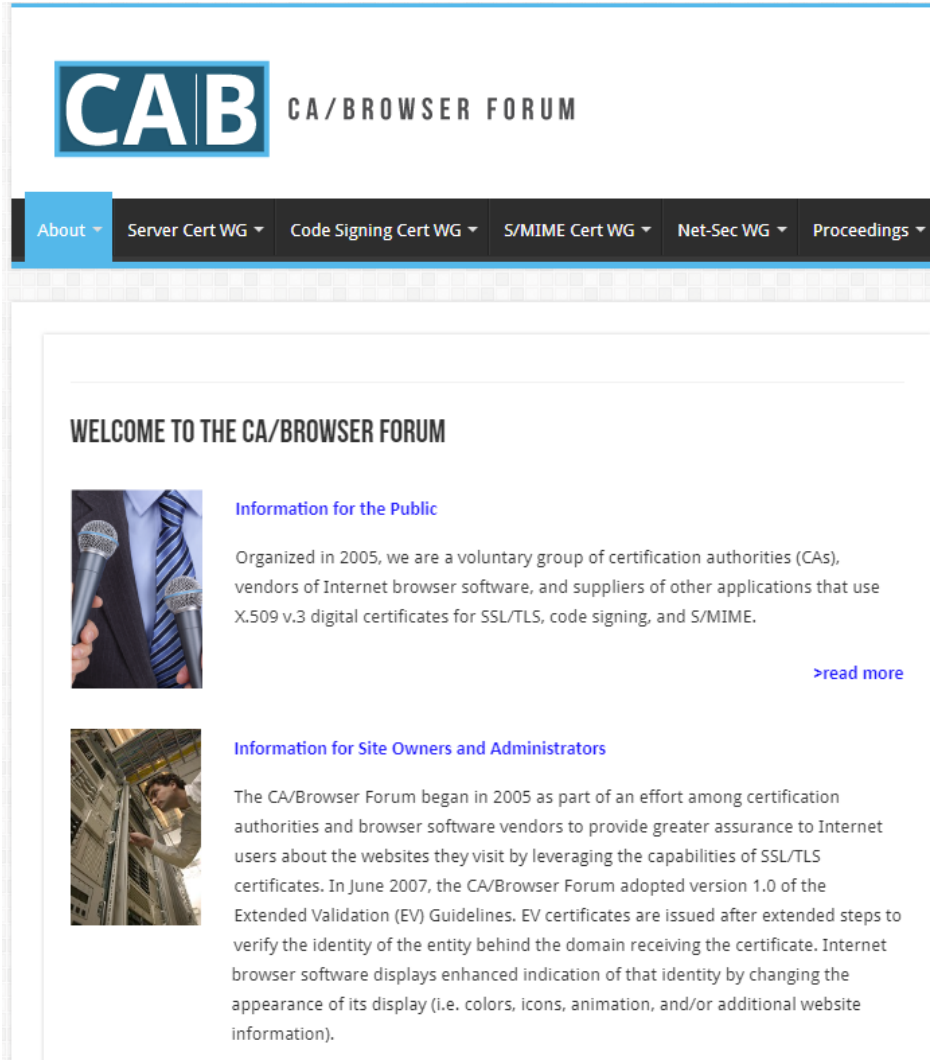
CA/Browser Forum



- 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

buypass

CA/Browser Forum - bakgrunn

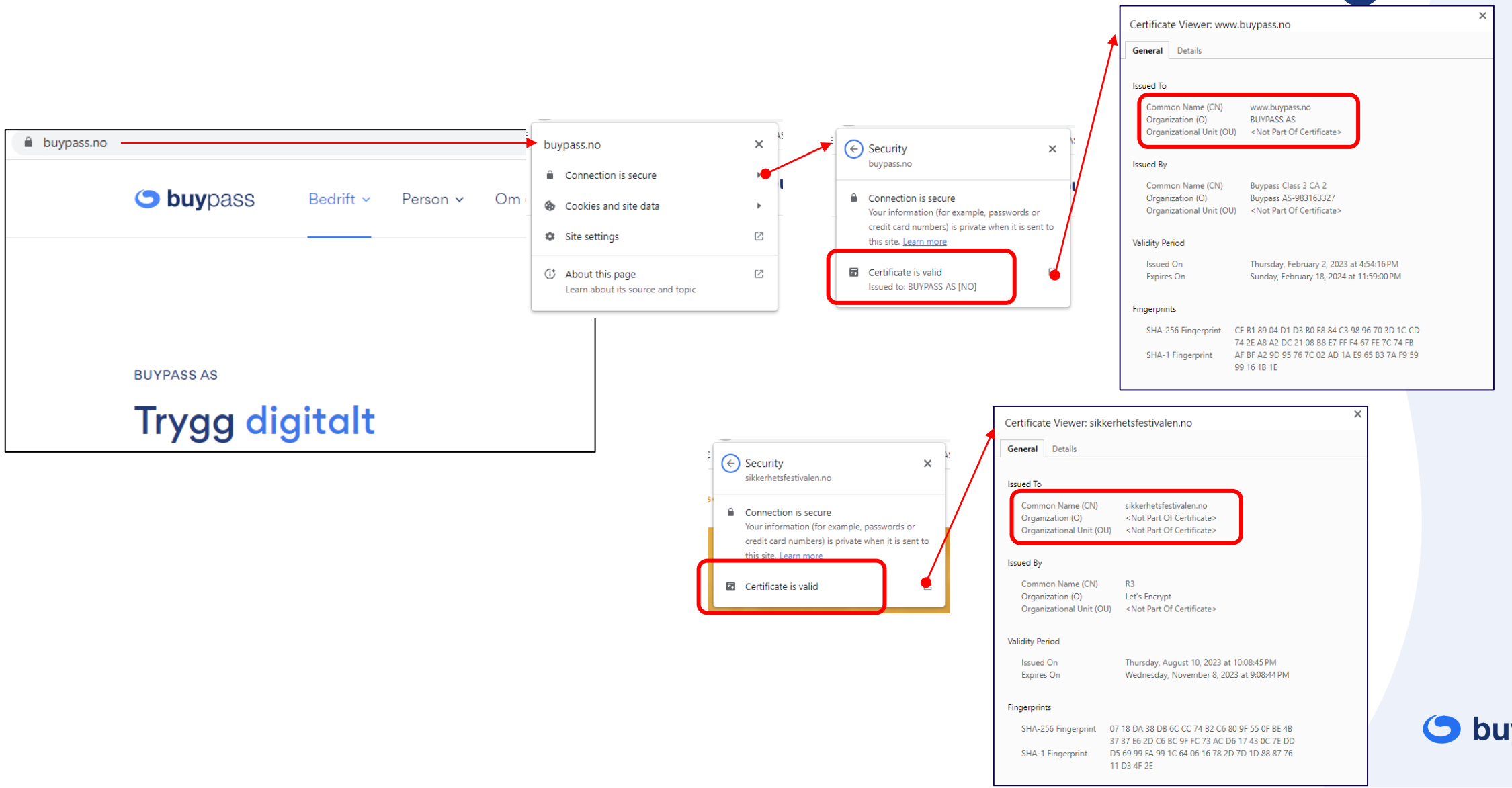


- Etablert i 2005
- Første standard i 2007 for utstedelse av Extended Validation (EV) sertifikater
  - Identitet var en viktig faktor sammen med omfattende kontroller for å gjøre det trygt på nett i en verden der det ellers var “vill-vest” tilstander
- Baseline Requirements i 2012
  - Minimumsnivå for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

buypass

Identitet i TLS-sertifikater – EV i går

Identitet i TLS-sertifikater – EV i dag



buypass

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	twitter.com
Organization	Twitter, Inc.
Location	San Francisco
State	California
Country	US

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

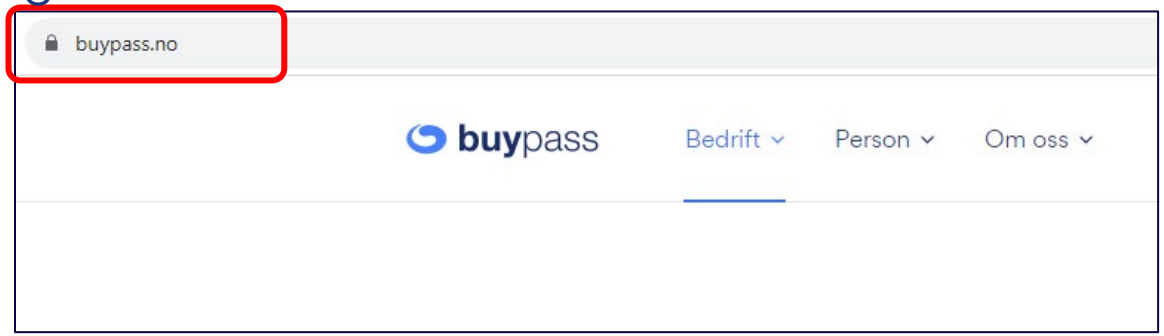
- **Users Don't Check.** The basic premise of EV is that users will look at the UI and behave differently when the EV indicator (the company name) is displayed. Unfortunately, this seems not to be the case. Chrome's Security team does a good job of summarizing the research in this area, but the TL;DR 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://educatedguesswork.org/posts/eidas-article45/

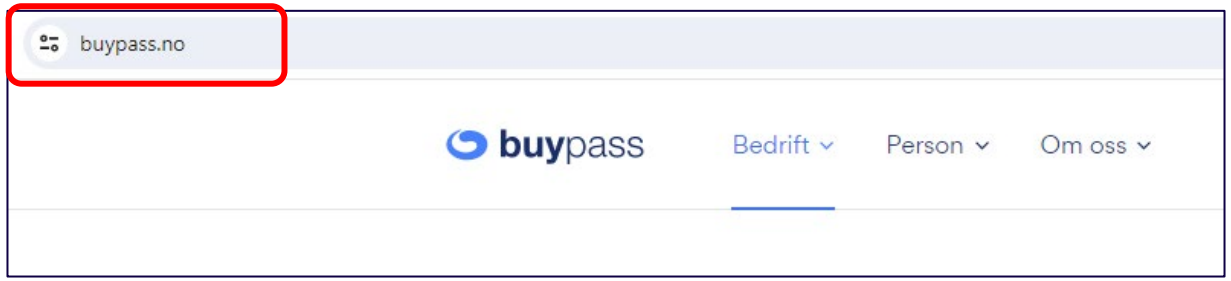
buypass

HTTPS i dag og i morgen (Chrome)

I dag:



I morgen:



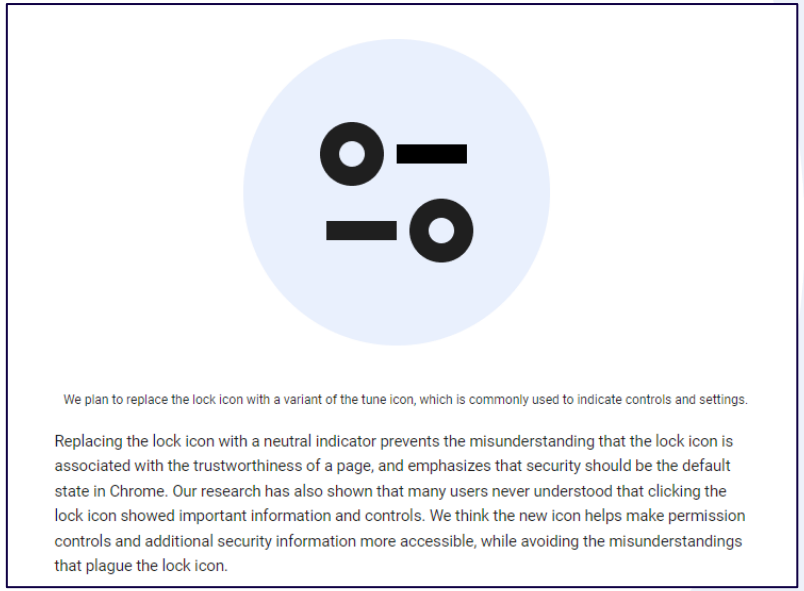
Chromium Blog

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.

buypass

eIDAS 2.0

QWAC: Qualified Website Authentication Certificate

buypass

eIDAS-forordningen

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

o

for electroni

and re

buypass

Buypass som tilbyder av tillitstjenester

eIDAS compliant
Qualified
Trust Service Provider

European Commission | EU Trust Services Dashboard

DISCOVER BROWSE TRY

CEF eSignature / EU Trust Services Dashboard / Browse / Trusted Lists / Norway / Trust service provider

Buypass AS

Trust services

QCert for ESig Qualified certificate for electronic signature

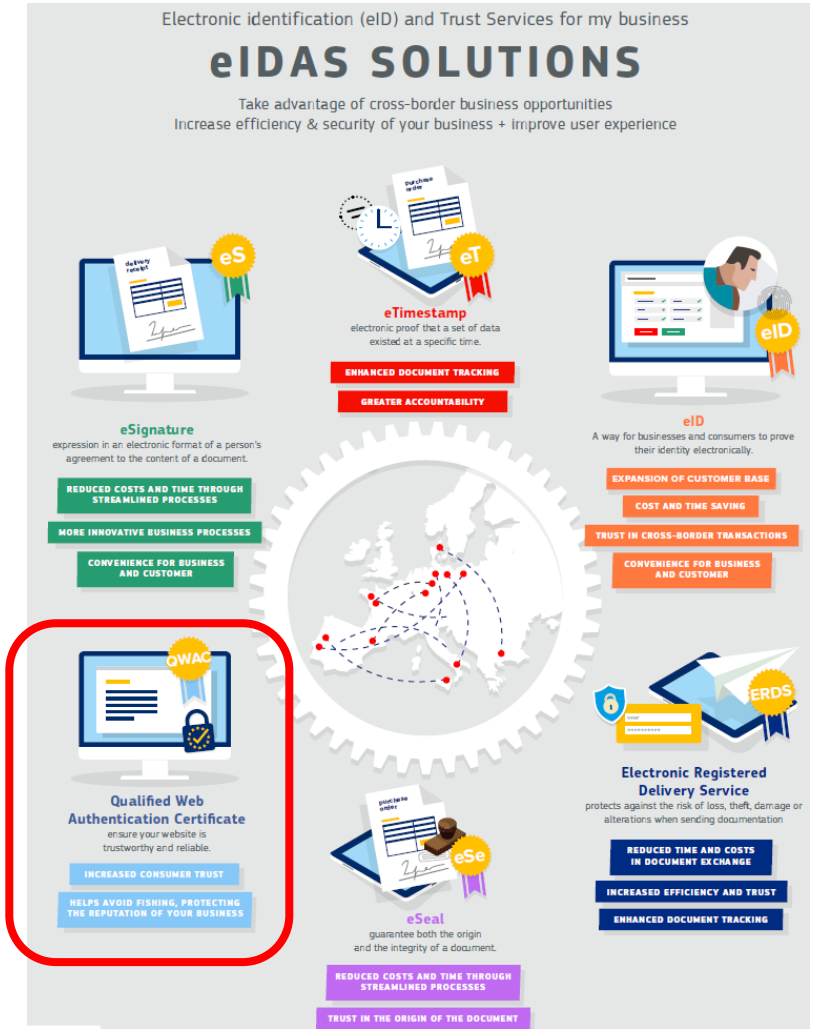
QCert for ESeal Qualified certificate for electronic seal

QWAC Qualified certificate for website authentication

Detailed information

buypass

QWAC – et kvalifisert TLS-sertifikat



- 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

buypass

Lovforslag 3.juni 2021 => eIDAS 2.0

EUROPEAN
COMMISSION

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 identitets-rammeverk og digital lommebok
- Men også enkelte andre viktige endringer
  - QWAC i artikkel 45

buypass

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).';

buypass

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 nettlesere til å samarbeide om dette, men dette har feilet**
  - Nettleserne har tvertimot gått i en helt annen retning og gjort tilgang på identitetsinformasjon mindre tilgjengelig for sluttbrukere de seneste årene

buypass

Forslaget møter motstand

Mozilla Campaign: securityriskahead.eu

KW

dev-security-pol

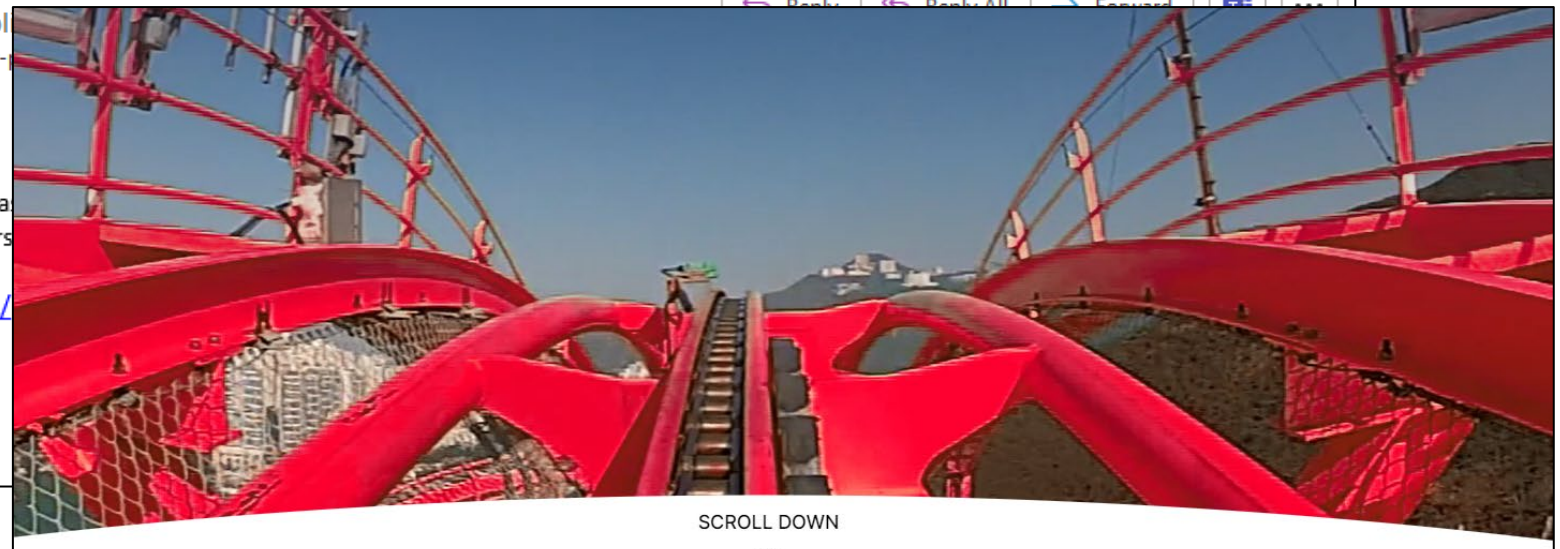
To dev-security-

All,

This is just FYI that Mozilla ha
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.

buypass

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 rotsertifikatprogrammenes 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

buypass

Men argumentene møter motstand

European Signature Dialog

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."

THE FACTS:

THESE STATEMENTS ARE **FALSE**

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.

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.**"*

THE FACTS:

VERY MISLEADING

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.

buypass

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.

buypass

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 nettlesere 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**

buypass

Vil identitet få sin renessanse?

buypass

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

buypass

Spørsmål?

buypass