스마트 씰(Smart Seal)과 함께하는 사이버 보안 및 소프트웨어 공급망 관리를 위한 제안

DigiCert Korea

나 정주 지사장

(Country Manager for Korea, Indonesia, Pakistan and Vietnam)

James.Nah@digicert.com

Agenda

- **DigiCert** 소개
- **TLS / SSL** 인증서
- **TLS / SSL** 인증서 시장
- 디지서트 스마트 씰(**Smart Seal**)
- 소프트웨어 공급망을 위한 보안 – **SSM(Secure Software Manager)**
- **Q&A**

DigiCert 회사 소개

digicert®

DigiCert – 혁신과 리더쉽의 역사

1995

VeriSign becomes the first Certificate Authority

VeriSign Secured

2003

DigiCert founded based on the question, "Isn't there a better way?"

digicert

2007

DigiCert partners with Microsoft to develop first Multi-Domain certificate

domain
domain
domain

2013

DigiCert builds first CT log accepted by Google

2016

DigiCert acquires Verizon SSL/TLS business

verizon

2018

DigiCert's trusted roots become encryption foundation for enterprises worldwide

Verify > digicert SECURED

1997

VeriSign becomes first international CA

2005

DigiCert becomes founding member of the CA/Browser Forum

CAB CA/BROWSER FORUM

2010

Symantec acquires Verisign Authentication

Norton SECURED powered by Symantec

2015

DigiCert launches scalable IoT platform

IoT

2017

DigiCert acquires Symantec's Website Security business

Norton SECURED Certified by digicert

2019

DigiCert acquires QuoVadis CA

QuoVadis

DigiCert – TLS/SSL 인증서와 IoT 보안 선도 기업

- 1등 Enterprize TLS/SSL 인증서 업체
- "Frost & Sullivan" awarded as "2020 Global TLS Certificate Company of the Year"
- "Fortune 500"의 89%와 Top 100 banks의 97%가 선호
- 매일 260억 개의 Web connection의 안전한 연결 보장
- 디지서트가 보호하는 글로벌 e커머스 트랜잭션 비중이 87%
- TLS/SSL, PKI & IoT 솔루션을 전세계 180여개국에서 제공
- Automation platform 인 "DigiCert One", "CertCentral" 발표
- 2018년 10월 DigiCert-Gemalto-Isara 등 3사가 양자 컴퓨팅 시대의 미래 사물인터넷(IoT) 보안을 위한 파트너십 체결
- 세계 최초 "PQC test kit" 발표(DigiCert Secure Site Pro)

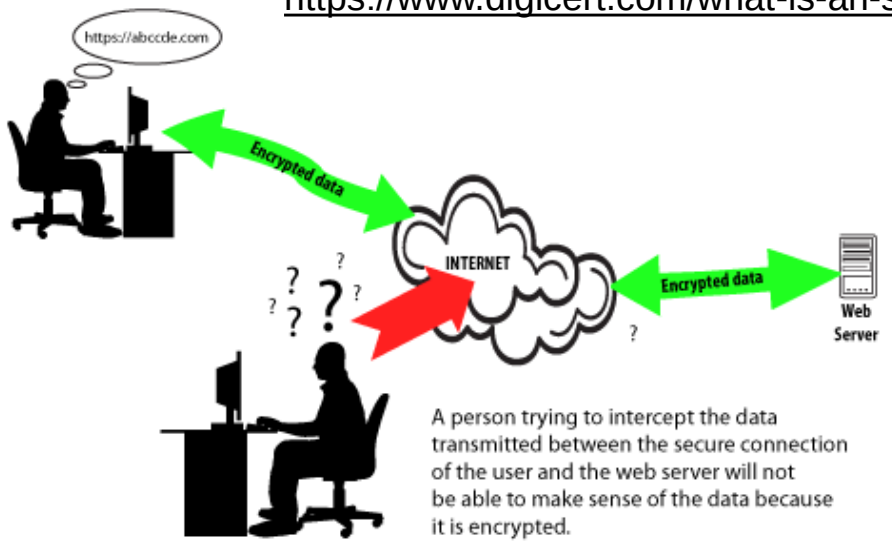
"Based on Forbes Global 2000 list published in 2017/Fortune 500 2017 and internal customer analysis conducted in October 2017, Frost & Sullivan 2019

TLS / SSL 인증서

digicert®

TLS(Transport Layer Security) / SSL(Secure Socket Layer) 인증서란?

https://www.digicert.com/what-is-an-ssl-certificate



TLS인증서는, Web server와 User간의 Authentication, Encryption, Integrity를 제공

사용자와 웹 서버 간의 데이터는 암호화되어 있기 때문에 중간자가 공격하여 Data를 보더라도 내용을 알 수 없음

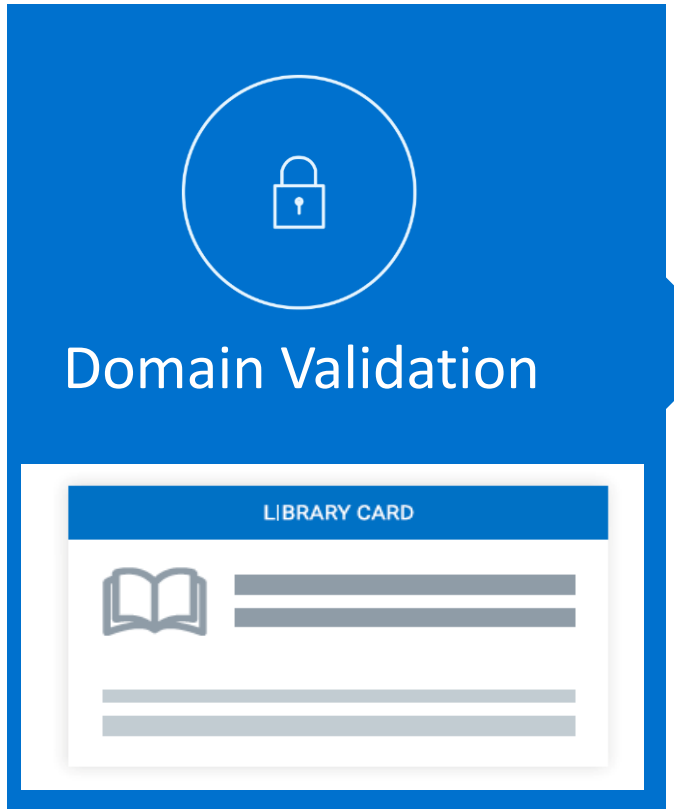
TLS인증서는 고객사의 Web서버 담당자가 CSR(Certificate Singing Request)을 서버에서 생성 후, CA(Certificate Authority, 공인인증 기관)에 제출하여, 신청 됨

TLS 인증서는 Public key와 Private key 그리고, Subject으로 구성됨

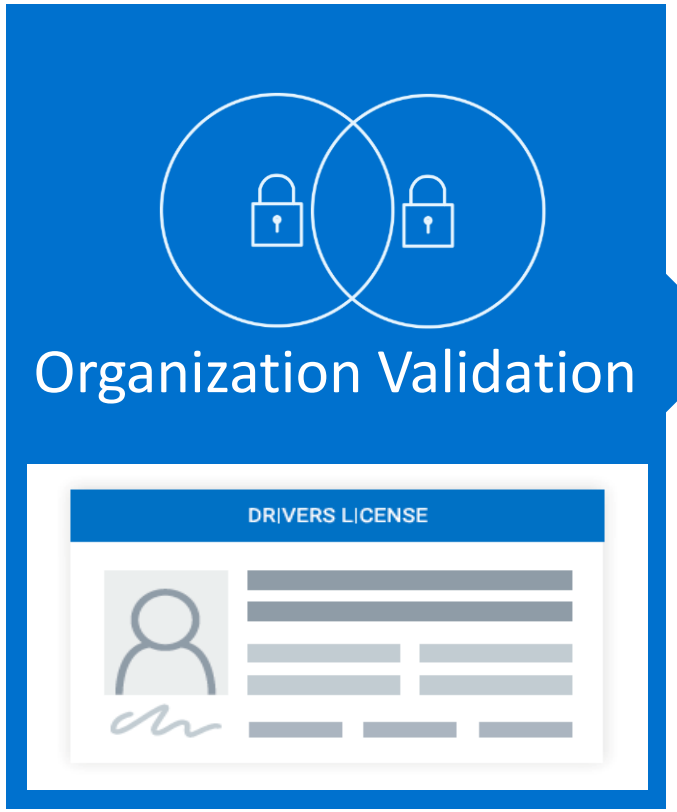
CA는 브라우저와 CA 간의 기관인 CAB Forum에서 인정 받아야 하며, 매년, Webtrust audit을 받아야 함

SSL은 SSLv3.0까지 였고, 현재는 SSLv4.0 대신 TLSv1.0로 명명되었고, 현재는 TLSv1.3

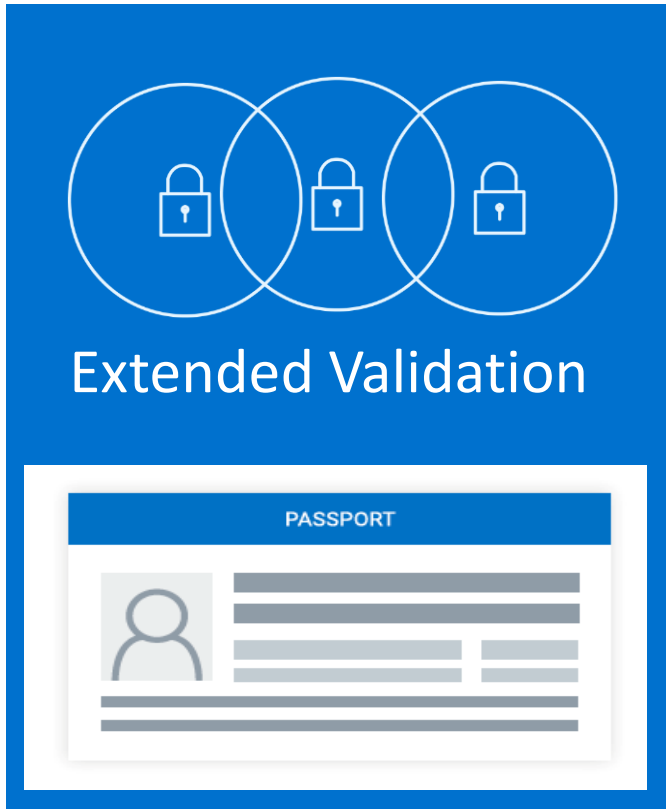
인증서 종류 - A Helpful Analogy



RapidSSL GeoTrust powered by digicert thawte powered by digicert



digicert GeoTrust powered by digicert thawte powered by digicert

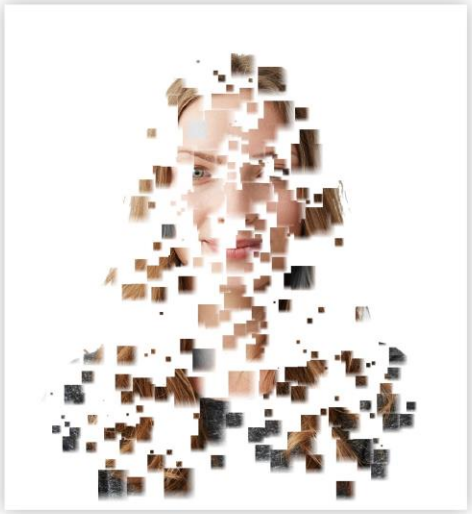


digicert GeoTrust powered by digicert thawte powered by digicert

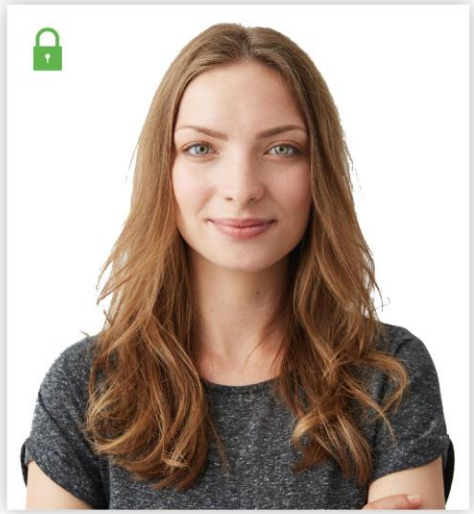
인증서 종류 - A Helpful Analogy

Give customers a clearer picture of who you are

Domain Validated (DV) certificates provide the lowest level of authentication, meaning anonymous entities can get a certificate. Jane Does meander at this level.



Organization Validated (OV) certificates provide additional checks to ensure brand protections. Jane Doe can no longer hide in the shadows at this level.



Extended Validation (EV) certificates guarantee the highest standard of brand protections. With EV, brands signal a commitment to customers that transactions are secure. Jane Doe is thoroughly identified.

인증서 종류 – 인증 절차에 따른 구분

Domain Validation

- Provides
  - Encryption
  - Validation of domain control
- Issued in minutes

RapidSSL GeoTrust powered by digicert thawte powered by digicert

Organization Validation

- Provides everything in DV, plus…
  - Authentication of organization
  - Proof of applicant's right to request cert for domain
  - Org details in Certificate info
- Issued in hours

digicert GeoTrust powered by digicert thawte powered by digicert

Extended Validation

- Provides everything in OV, plus…
  - Stringent, industry-standardized authentication of organization
- Issued in about a day

digicert GeoTrust powered by digicert thawte powered by digicert

인증서 종류 – DV, OV, EV 중 어떤 인증서를 사야 하나요?

Domain Validation

- Browser compliance
- Informational pages
- Just need encryption
- Price sensitive customers

GeoTrust powered by digicert RapidSSL thawte powered by digicert

Organization Validation

- Pages requiring sensitive info (passwords, payment details, etc.
- Wants more than just encryption

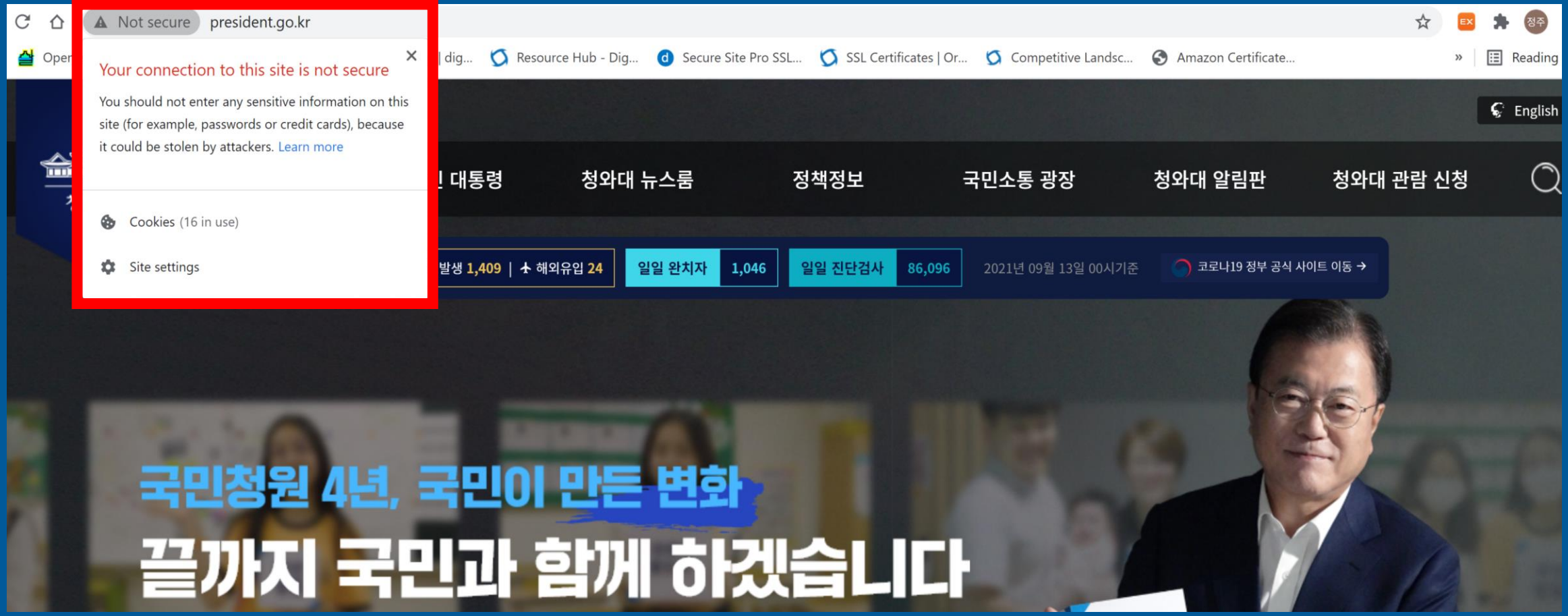
digicert GeoTrust powered by digicert thawte powered by digicert

Extended Validation

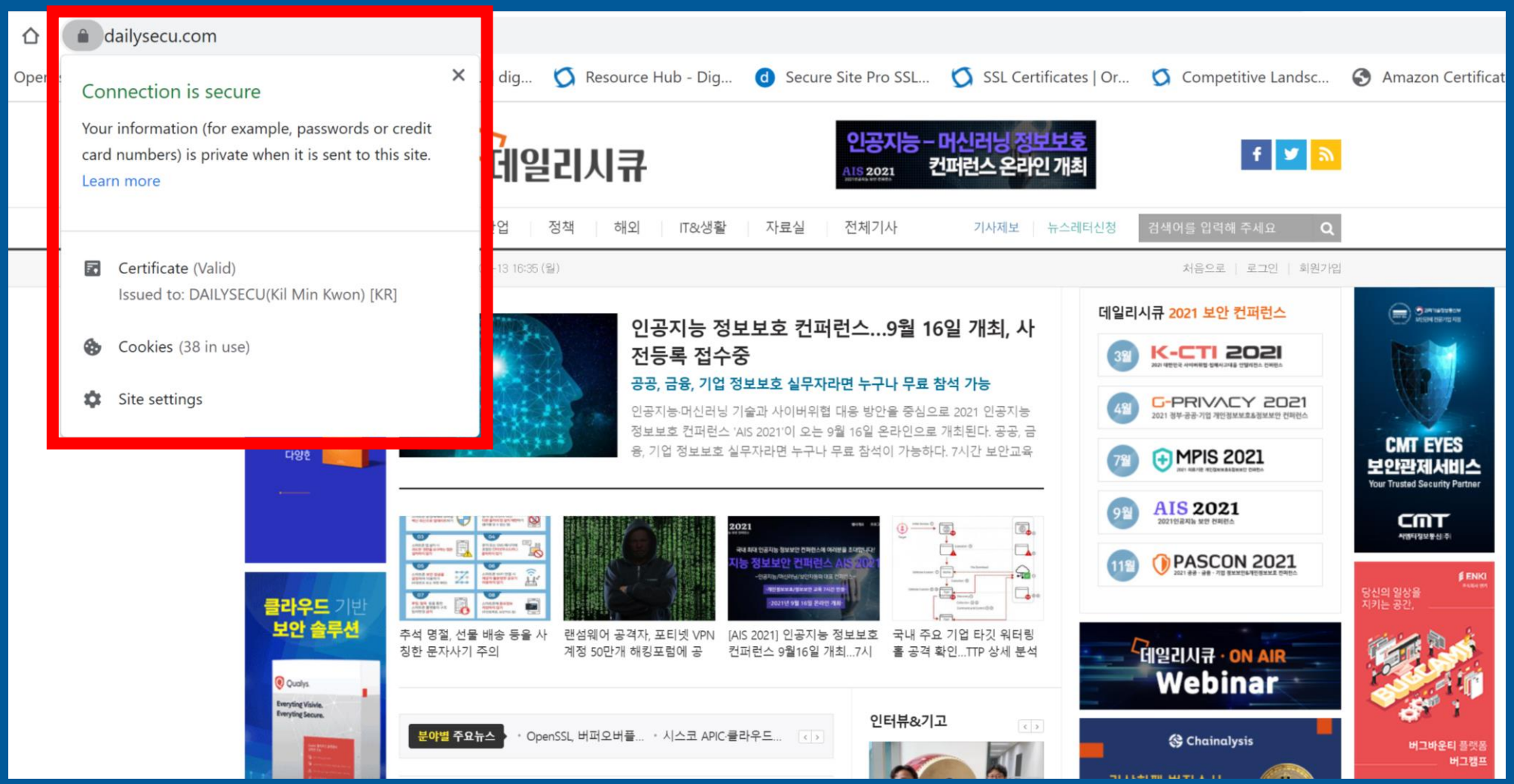
- Ecommerce
- Online banking
- Serious about security
- Security messaging important

digicert GeoTrust powered by digicert thawte powered by digicert

TLS / SSL 인증서가 없는 경우



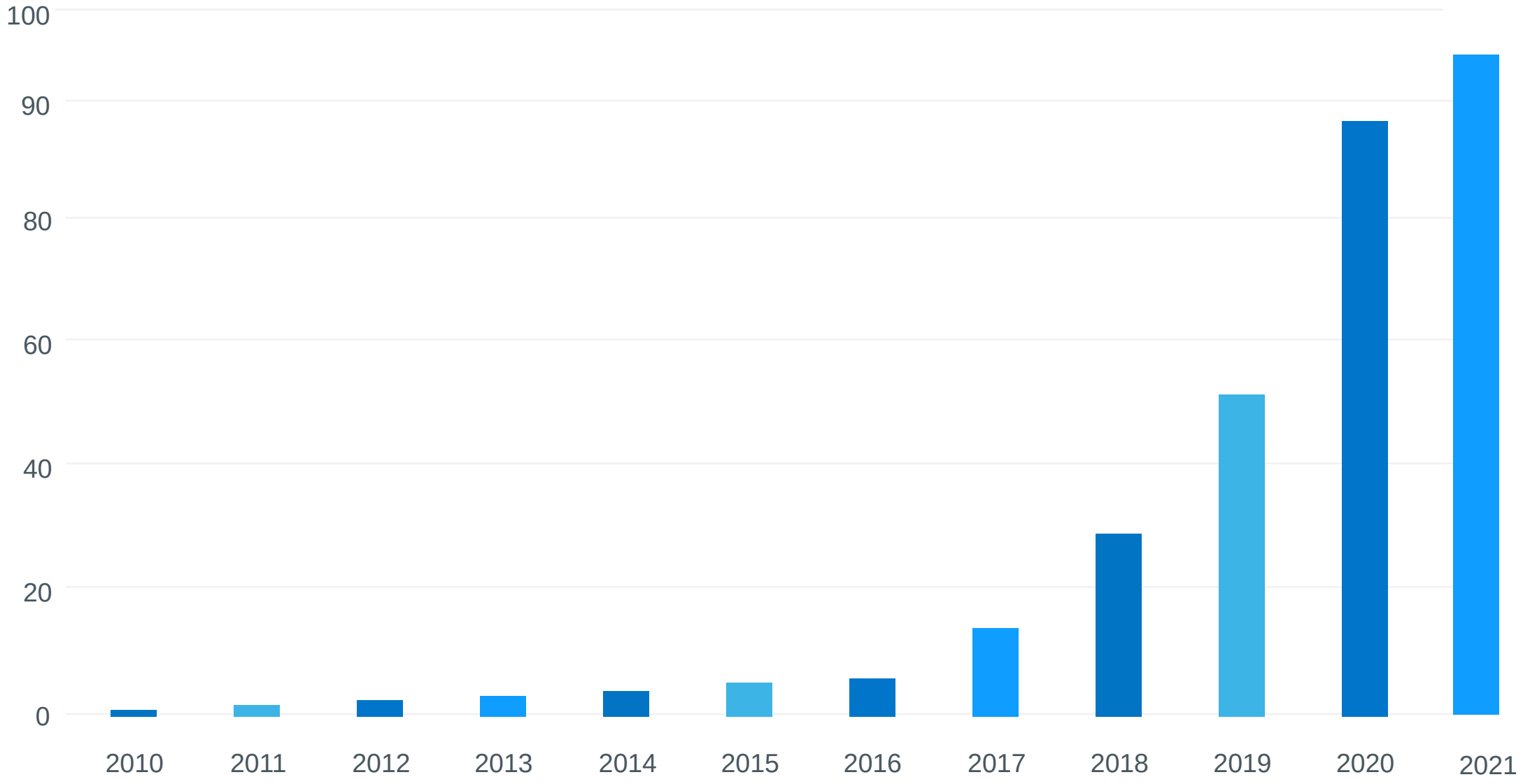
TLS / SSL 인증서(EV)가 있는 경우



TLS / SSL 인증서 시장 - 전세계

digicert®

TLS Certs over Time



The World of Publicly Trusted TLS (according to Netcraft) June 2021

95M

95M certs observed by Netcraft

1.6M

Up 1.6M certs from last month

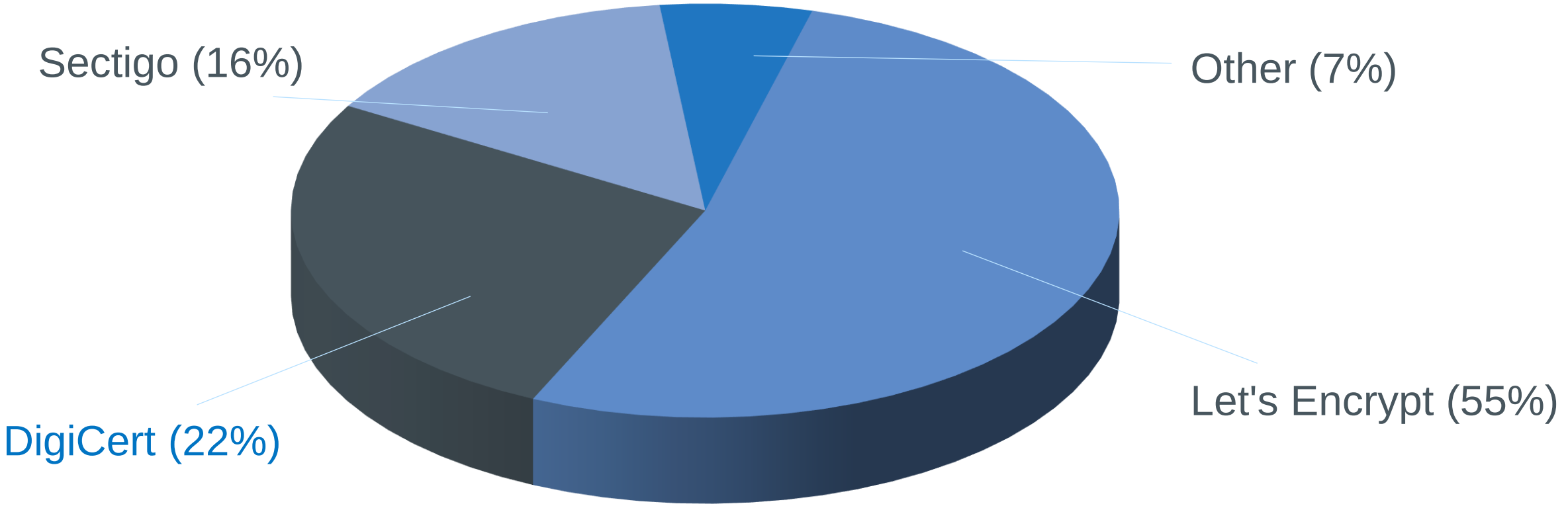
1.2M

DigiCert has 1.2M new certificates since Feb 2021

21.8M

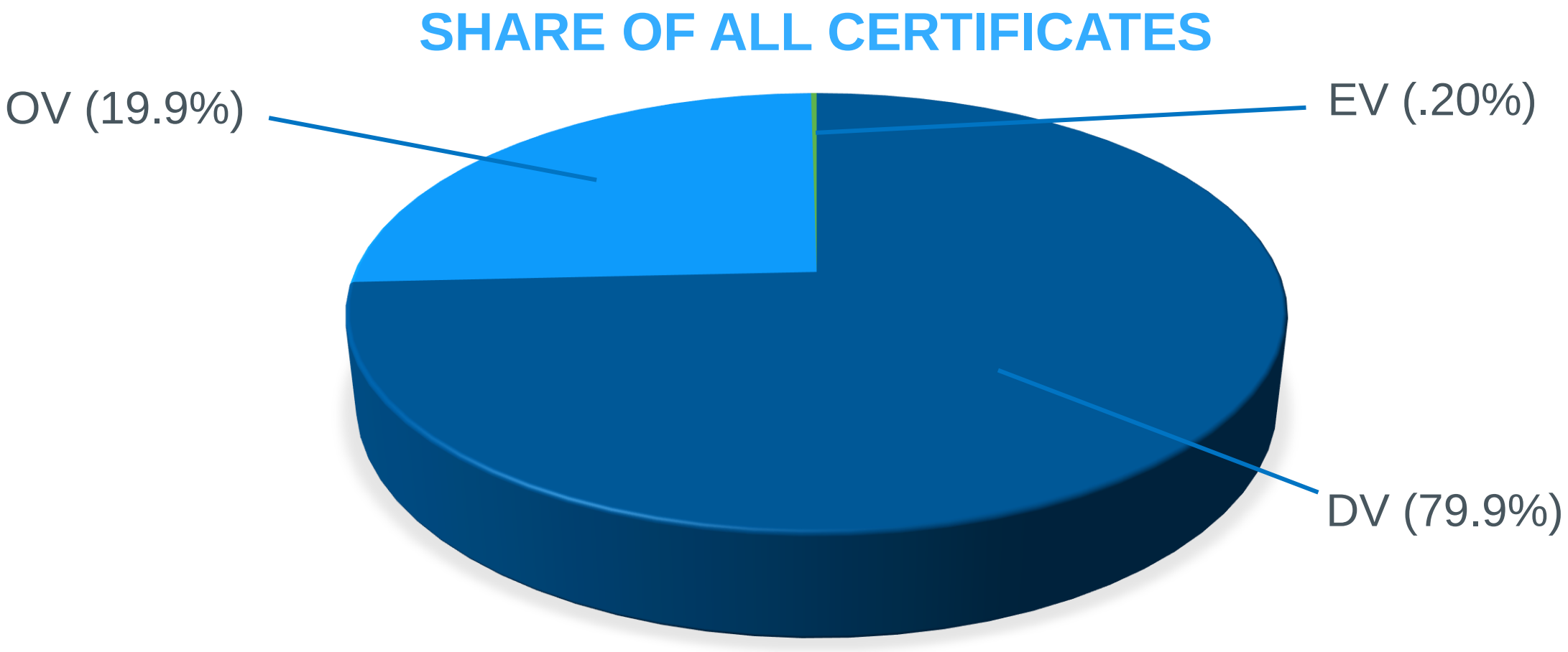
DigiCert with 21.8M active certs (nearest competitor has 15M)

Total Share of Certificates – June 2021

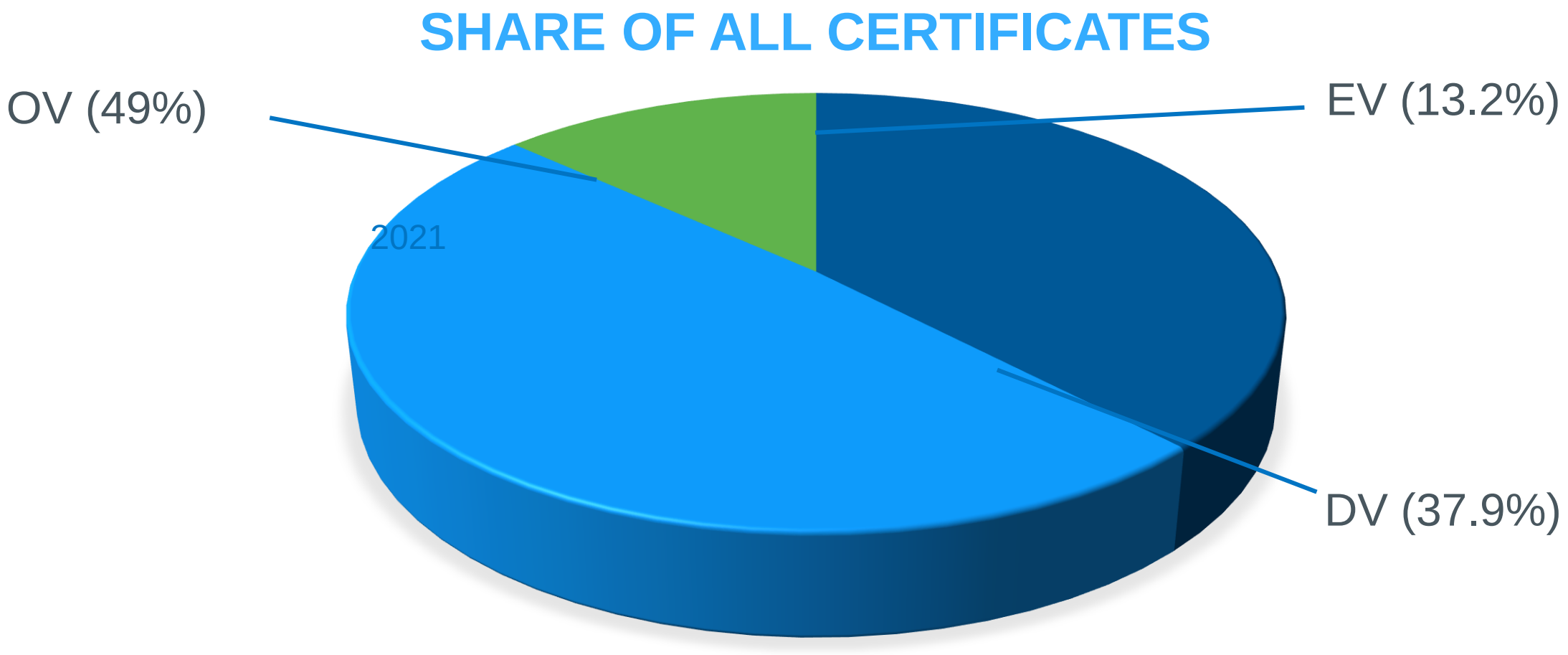


Total: 95,407,259

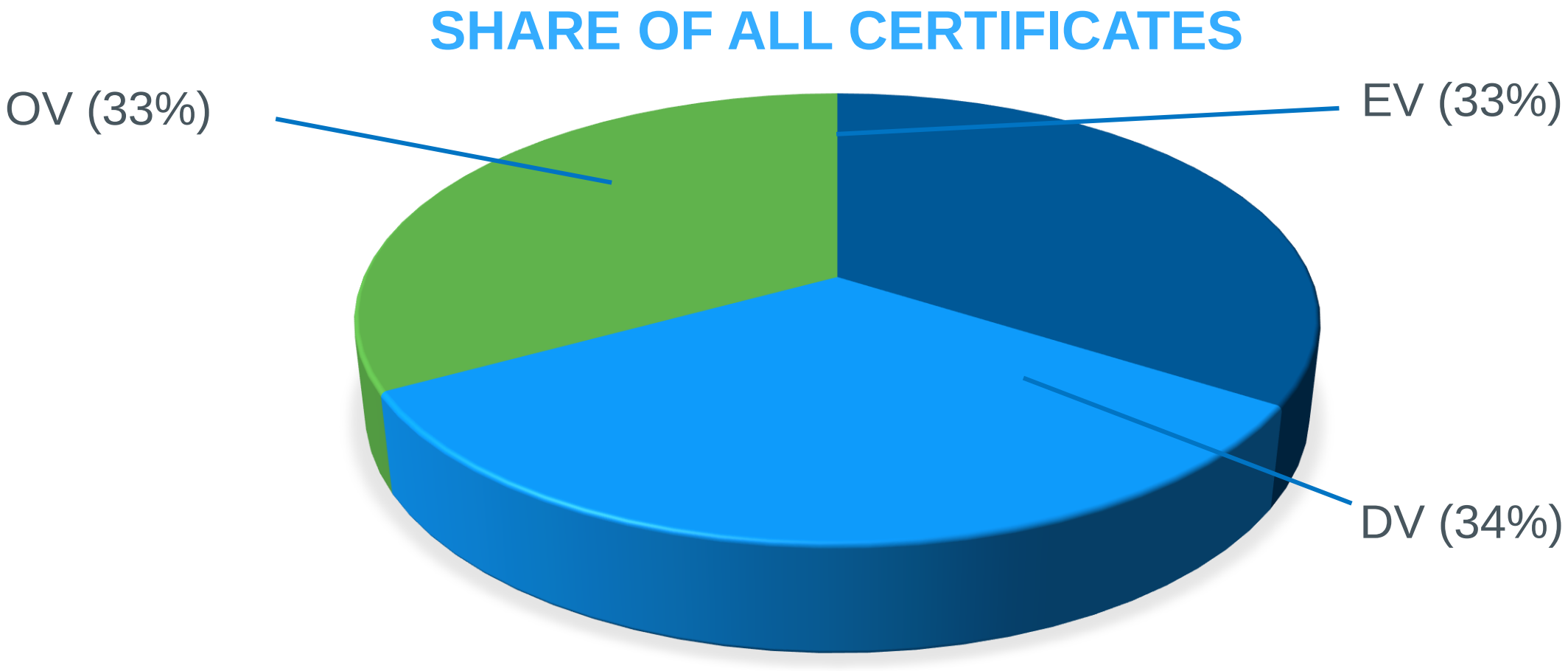
% by Certificate Type – Mar 2021



SHARE OF TRAFFIC BY PRODUCT TYPE– Mar 2021



SHARE OF ECOMMERCE TRANSACTIONS BY CERT TYPE– Mar 2021



TLS / SSL 인증서 시장 - 한국

digicert®

2020년10월 국정감사에서 이슈가 된 공공기관 TLS/SSL 인증서

데일리시큐

이슈 | 산업 | 정책 | 해외 | IT&생활 | 자료실 | 전체기사 | 기사제보 | 뉴스레터신청

최종편집 : 2021-07-08 10:15 (목)

HOME > 정책 > 긴급속보

행안부, HTTPS-Only 정책 도입 및 정부발급 인증서 구축 계획 수립

길민권 기자 | 승인 2020.10.26 16:26

행안부, 10월 말까지 정부부처·지자체·공공기관 웹페이지 3만 여 개 전수조사 완료

행정안전부가 전부처·지자체·공공기관을 포함한 전수조사를 통해 HTTPS-ONLY(모든 정부부처 및 지자체 홈페이지에 HTTPS도입)정책 도입 및 정부발급 인증서 구축 계획을 밝혔다.

지난 7일 행정안전부 국정감사에서 김영배 더불어

ZDNet Korea 뉴스 | 이슈진단+ | 컨퍼런스 | 칼럼 · 연재 | 포토 · 영상

행안부, 전체 공공 사이트에 HTTPS 도입 검토

김영배 의원 "보안 최신 동향 반영토록 전자정부법 개정 추진"

컴퓨팅 | 입력 :2020/10/27 17:03 수정: 2020/10/27 17:06

김윤희 기자 | 기자 페이지 구독 | 기자의 다른기사 보기

[웨비나] 다양한 환경에서 운영할 수 있는 지능형 관제시스템의 적용방법을 소개합니다!

행정안전부가 중앙부처, 지방자치단체, 공공기관의 인터넷 사이트에 HTTPS를 적용, 보안을 강화하는 방안을 검토한다.

27일 행정안전부 관계자는 이같은 정책을 검토하고 있다며 "전체 공공기관 웹사이트를 전수조사한 결과를 보고 자세한 방향을 결정할 계획"이라고 밝혔다.

웹사이트 이용자와 웹 서버 간 통신을 주고 받게 해주는 프로토콜로 HTTP가 있다. 그러나 HTTP는 주고 받는 데이터가 암호화돼 있지 않아 보안에 취약하다는 지적이 있어왔다. HTTPS는 이를 보안소켓계층(SSL)을 통해 암호화한 것이다.

행안부는 과거 공공기관 웹사이트의 HTTPS 적용을 지원해왔다. 그러나 정부 발급 SSL(G-SSL) 인증서 기반 공공

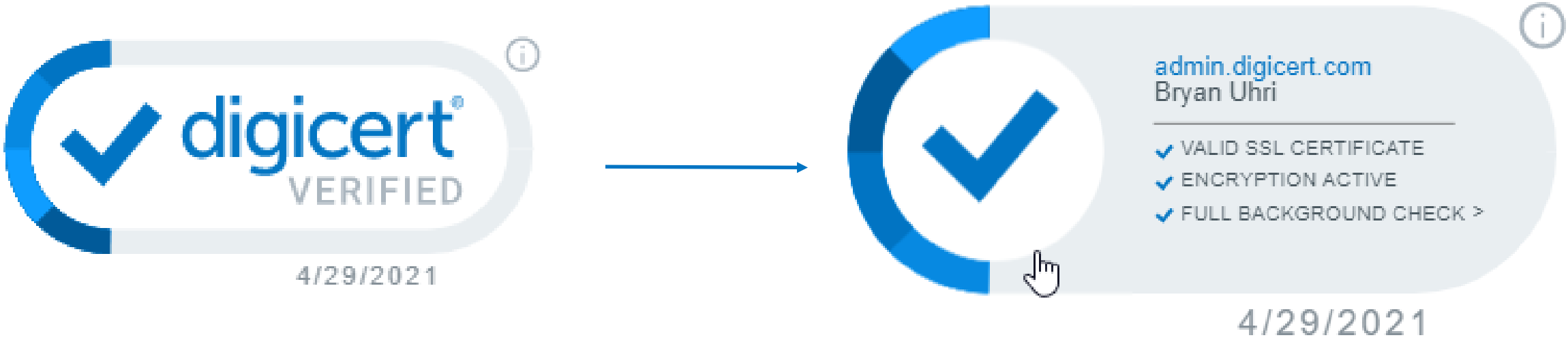
데일리시큐: https://www.dailysecu.com/news/articleView.html?idxno=115540

디지서트 스마트 씰(Smart Seal)

digicert®

디지서트 스마트 씰 – The Next Generation Site Seal

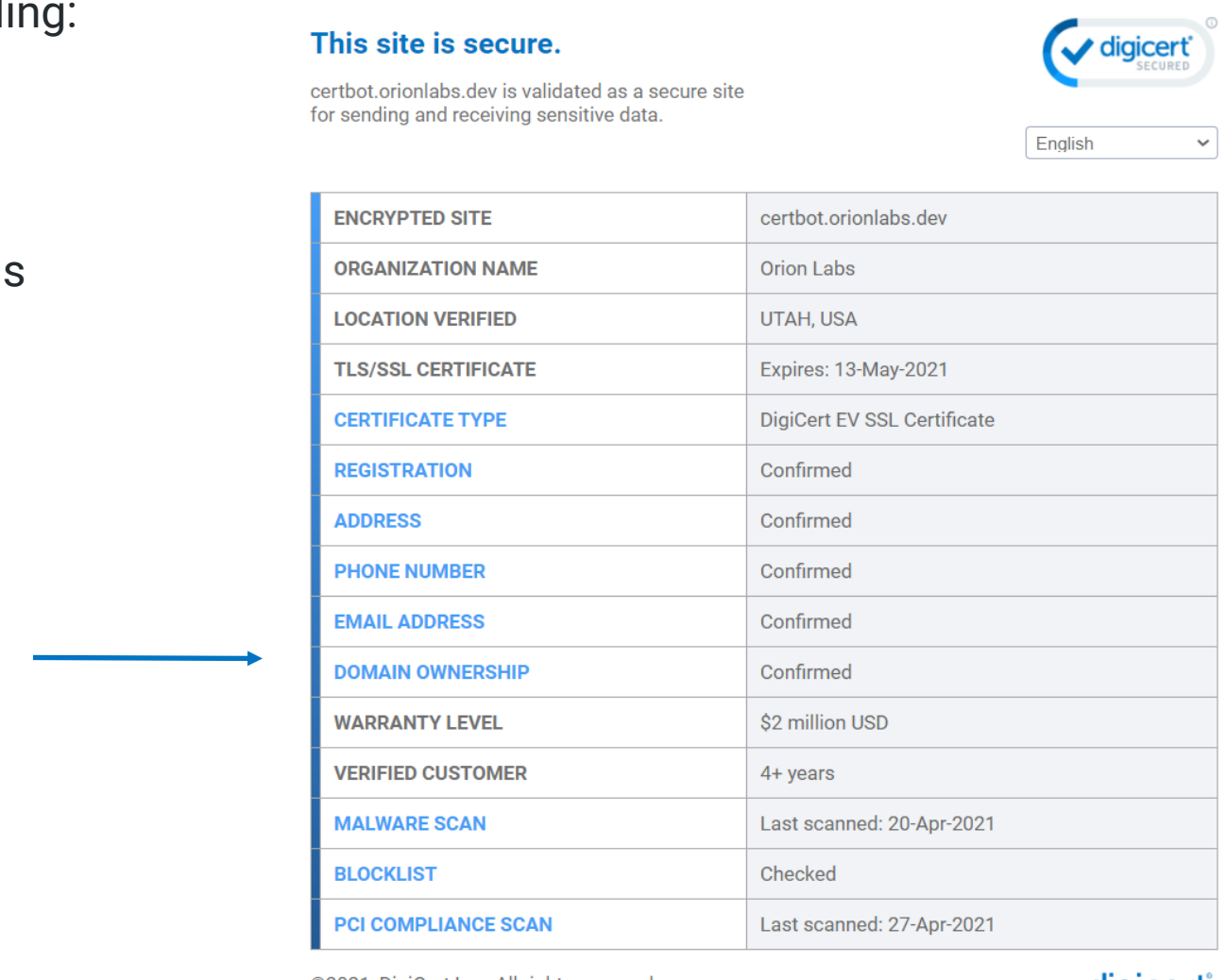
- April 2021 - Introducing the next generation site seal – available with all **Secure Site** and **Secure Site Pro** certificates
- Dynamic, with micro-interactions
- Difficult to copy, spoof or steal
- Rollover data provides quick information
- Easily recognize site has been validated
- Critical identity and security information



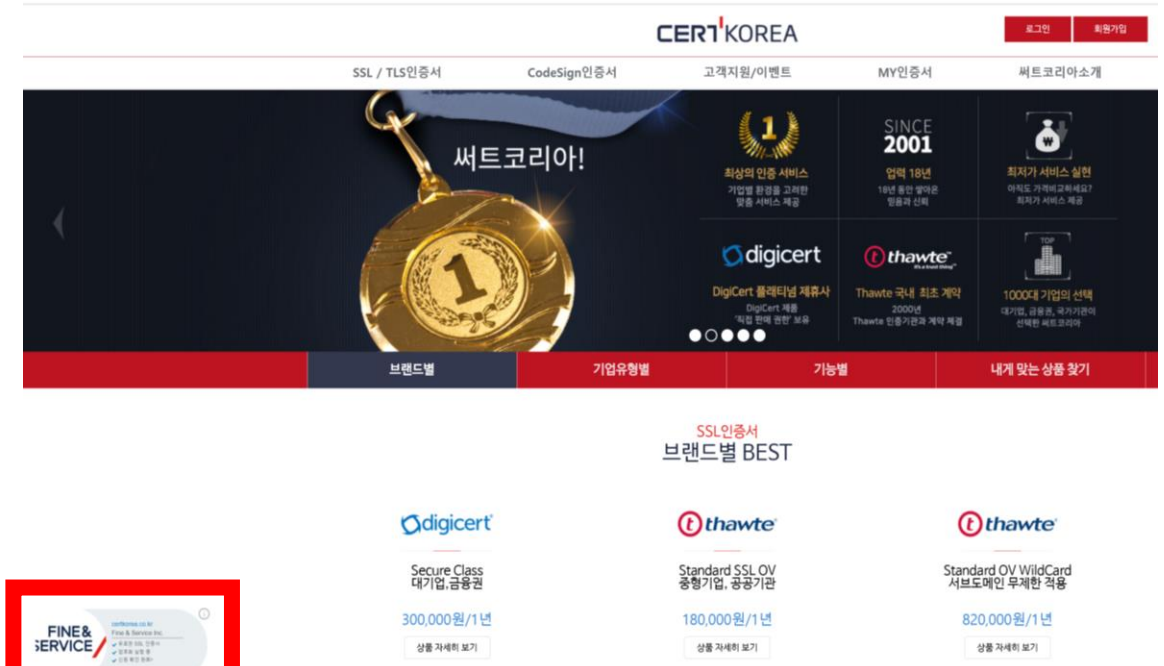
Smart Seal Video: https://vimeo.com/536632505

디지서트 스마트 씰 – Details

- Prominently displays information regarding:
  - ✓ Website
  - ✓ Identity
  - ✓ Brand
- Eye-catching, dynamic micro-interactions
- Company logo
- Details on extra security features



디지서트 스마트 씰 – (써트코리아: Certkorea.co.kr)



digicert

디지서트 스마트 씰을 써야하는 이유

1 INCREASE WEBSITE CONVERSIONS

Studies have shown that displaying a site seal on a webpage is effective at increasing conversions. A recent study shows sites that display site seals or trust marks perform 48% better than sites that don't, thus increasing conversion rates and increasing ROI.

2 DISPLAY TRUSTED AUTHENTICATION

Demonstrate that DigiCert, the world leader in high assurance TLS/SSL certificates has validated the site and is providing our industry-leading protection. It also verifies that an organization is properly securing its webpage and brand.

3 INTERACTIVE & ENGAGING

When users hover over the DigiCert Smart Seal, certificate information will be magnified through micro-interactions. The seal will also produce an information page when clicked on, with details including company name, address/location, date issued and level of encryption.

4 BOOST BRAND CREDIBILITY

Site seals help startups and growing businesses prove that they're an established and credible business. Established brands benefit too by aligning their brand with the leading TLS provider in the market, and further showing that the user is on the legitimate site.

5 INCREASE USER CONFIDENCE

The dynamic animation within the seal draws from real-time DigiCert certificate data and gives site visitors assurance that the website is proactively protecting their data. The Smart Seal code will actively call back to DigiCert systems for updated information.

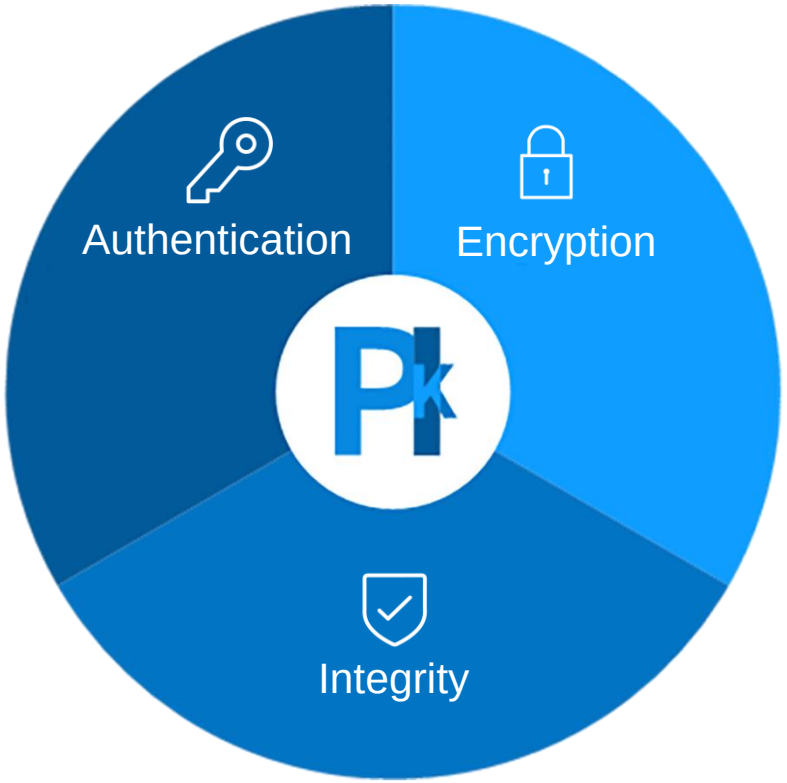
https://www.digicert.com/tls-ssl/digicert-smart-site-seal

소프트웨어 공급망을 위한 보안 – 디지서트 SSM (Secure Software Manager)

digicert®

Code Signing이란 무엇인가?

Code signing is a method to confirm that code or other digital binaries have not been altered



Authentication(인증)

Proves that you are who you say you are
Creates trust and drives accountability

Encryption(암호화)

Uses public-private keypair to sign code and compare hashes
Substantiate the identity of the file owner and file integrity

Integrity(무결성)

Verifies that the file has not been tampered
Minimizes malware propagation via unsigned file downloads

왜 Code Signing이 필요하죠?

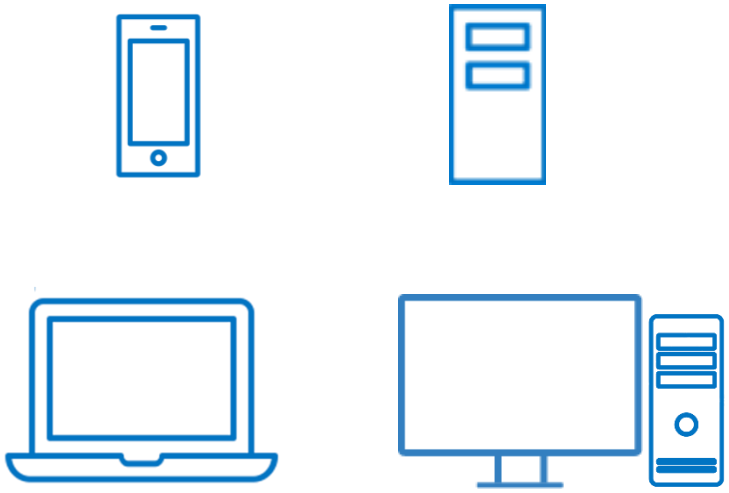
Minimize Malware Downloads

Stay in Compliance

Avoid Security Warnings

Code Signing: 예전에는…

DISTRIBUTION OF PLATFORMS, APPS AND SOFTWARE

10 YEARS AGO	
	
Code signing use cases	Devices

Code Signing: 오늘날에는…

EXPLOSION OF PLATFORMS, APPS AND SOFTWARE

TODAY

Connected Devices: 2018 - 70억개; 2020 – Projected 310억 개; 2025 - Projected 750억+ 개

Applications

Devices

전통적인 Code Signing의 취약점들

Signing keys are vulnerable to theft

Single signing key to sign all apps

No accountability for signing, and no rights management

No tracking of signing activity or auditing

SolarWinds 사례

데일리시큐

· 2021년 9월 16일 오전 9시~오후 5시
· 보안교육 7시간 이수 인정
· 공공, 금융, 기업 정보보호 실무자라면 누구나 무료 참석
AIS 202

이슈 | 산업 | 정책 | 해외 | IT&생활 | 자료실 | 전체기사 | 기사제보 | 뉴스레

최종편집 : 2021-09-13 18:25 (월)

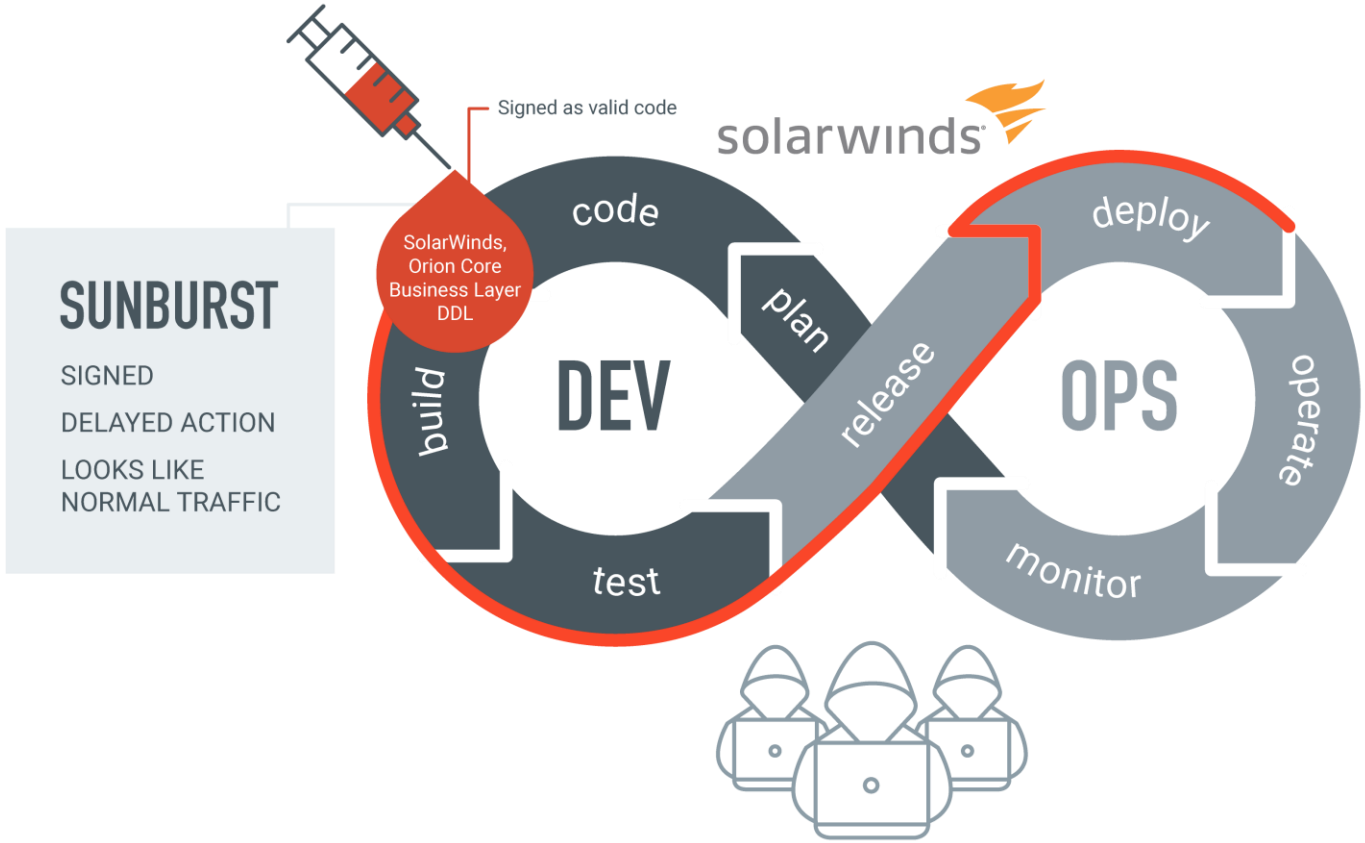
HOME > 이슈 > 외신

중국 해커, 솔라윈즈 취약점으로 美 국립금융센터 사이버공격

길민권 기자 | 승인 2021.02.05 12:23

중국과 연계된 것으로 추정되는 해커가 미 국립금융센터(NFC) 시스템을 공격하기 위해 솔라윈즈 오리온(SolarWinds Orion) 소프트웨어 취약점을 악용한 것으로 조사됐다고 시큐리티어페어스 등 외신들이 보도했다.

SolarWinds DevOps 프로세스



SolarWinds 결과

하기 **18,000**여 고객에게 영향을 줌

- Fortune 500 기업 중 425개 기업
- Top 10 미국 통신사
- 미 국방부
- 미 국무부
- 미 법무부
- 미군
- NSA(National Security Agency)
- 백악관

SolarWinds – 누구 잘못이죠?

정교한 헤커

Code signing

Code signing 제조사

CONTROLLED PROCESS의 부재

CISO 이 잘못해서

암호화 알고리즘

엔지니어들의 잘못

일반적인 Code Signing의 함정들

No mechanism for signing rights management	Uncontrolled distribution of signing key – unsecured USB	Using **THE SAME** signing key to sign all files	Using **THE SAME** signing key across different product lines and businesses	Having no reporting capability to show who signed what and when

디지서트 SSM(Secure Software Manager)

Secure Codesigning Workflows for Enterprise’s

Hash Signing

- Fast
- Secured IP

Account level security controls

- Validity
- Algorithms
- MFA

Private Key Protection

- Key workflows
- FIPs Compliance

Role-based Access Controls

- User management
- Separation of duties

디지서트 SSM(Secure Software Manager)

Traditional	Our Solution
Random or local key storage	Secure storage of signing keys in leading-edge technology including HSMs
No visibility on signing events	Full tracking and reporting on who signed what, when
No controls over who is signing what	Granular controls including permission and role-based access
Difficult to revoke certificates	Complete visibility and range of options available to act on keypairs and associated certificates
Manual integration with CI/CD process	Out-of-the-box integration with major CI/CD platforms
Limited support for file types and signing tools	All major file types and signing tools supported
Lack of deployment options	Flexible options for deployment: on-premises, public or private Cloud, or hybrid
Security risks and lag time with code signing in the Cloud	Hash signing expedites signing and reduces security risk


Q
&
A

digicert®

감사합니다.

digicert®

주요 고객사 * 국내1위 10,000 + 고객사가 선택 (2020년 기준)

DigiCert 관련 기사

전자신문, 디지서트 오토메이션 매니저: https://www.etnews.com/20210421000248

바이라인: https://byline.network/2021/04/22-123/

전자신문, 디지서트 공공기관 첫단추: https://www.etnews.com/20210304000158

데일리시큐, 디지서트 2021년 보안전망: https://www.dailysecu.com/news/articleView.html?idxno=116650

보안뉴스, CertCentral: https://www.boannews.com/media/view.asp?idx=90700

IT데일리, IoT: https://www.itdaily.kr/news/articleView.html?idxno=201653