

**THE MOST COLOSSAL CONFLICT THE SCREEN HAS EVER KNOWN!**

Vladimir Dzhuvinov

presents

**THE TRUST CHAIN**



**VS.**

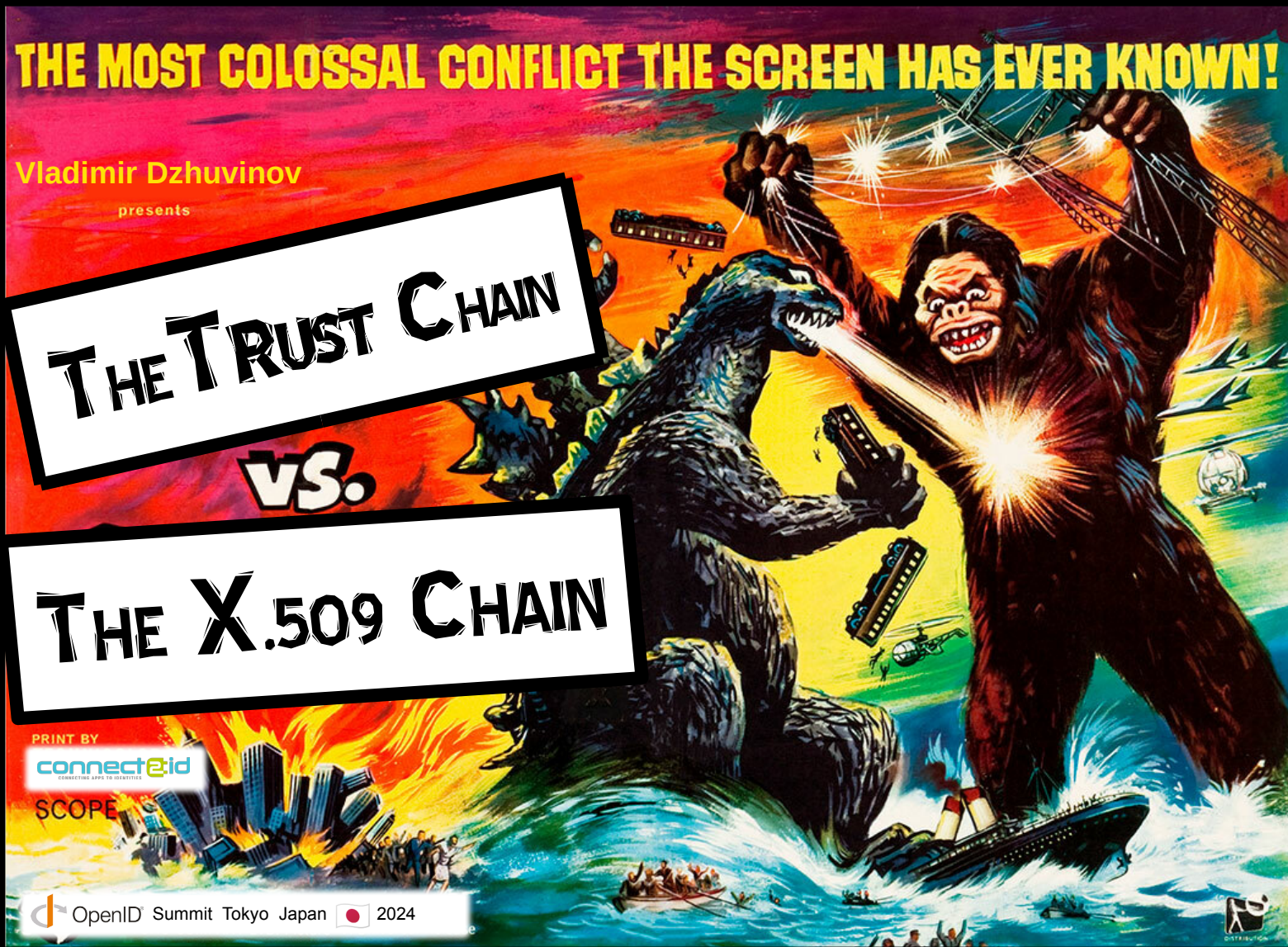
**THE X.509 CHAIN**

PRINT BY

**connect@id**  
CONNECTING APPS TO IDENTITIES

SCOPE

 OpenID Summit Tokyo Japan  2024

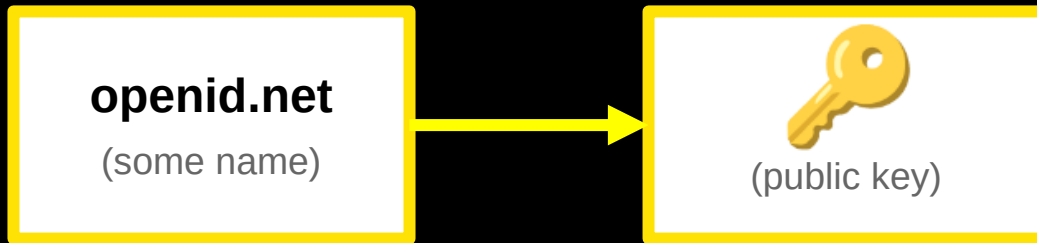


# 1988 – the year of the **X.509** certificate



- The 386 PC and the 1.44MB floppy disk become a hot thing
- **ASN.1** encoding is a hot thing
- The **WWW** is not a thing yet
- **HTTP** is not a thing yet
- **Web APIs** are not a thing yet
- **JSON** is not a thing yet
- **JWT** is not a thing yet

# Public key attestation with a X.509 certificate



The attestation is **signed** by a **trusted Certificate Authority (CA)**

Once the X.509 chain is validated the **public key** can be used  
to **verify signatures**,  
establish an **encrypted TLS channel**,  
etc.

# The **X.509** cert internals

- issuer
- subject

- not-before
- not-after

constraints



**public key**

# The Trust Chain JWT internals

- iss
- sub

- iat
- exp

constraints



**JWK set**



trust  
marks



entity  
metadata



metadata  
policies

# The Trust Chain vs the X.509 chain

	Trust Chain	X.509 chain
Attest public keys	V	V
Attest and police entity metadata	V	X
Complex trust topologies / federations	V	X
Include trust marks	V	X
Well-known URL & web APIs	V	X

2035

**TLS 2.0 adopts the OpenID Trust Chain  
for the benefit of all mankind**



# 2035

https://openid.net

< **Connection security and trust for openid.net**

**You are securely connected to this site.**

Domain verified by: **Let's Encrypt**

Legal entity verified by IRS USA: **OpenID Foundation**

**Trust marks:**

- Bank of America account holder
- ISO/IEC 27000 compliant
- Carbon neutral business
- Staff underwent Mars survival training

**DISCOVER**  
What is OpenID

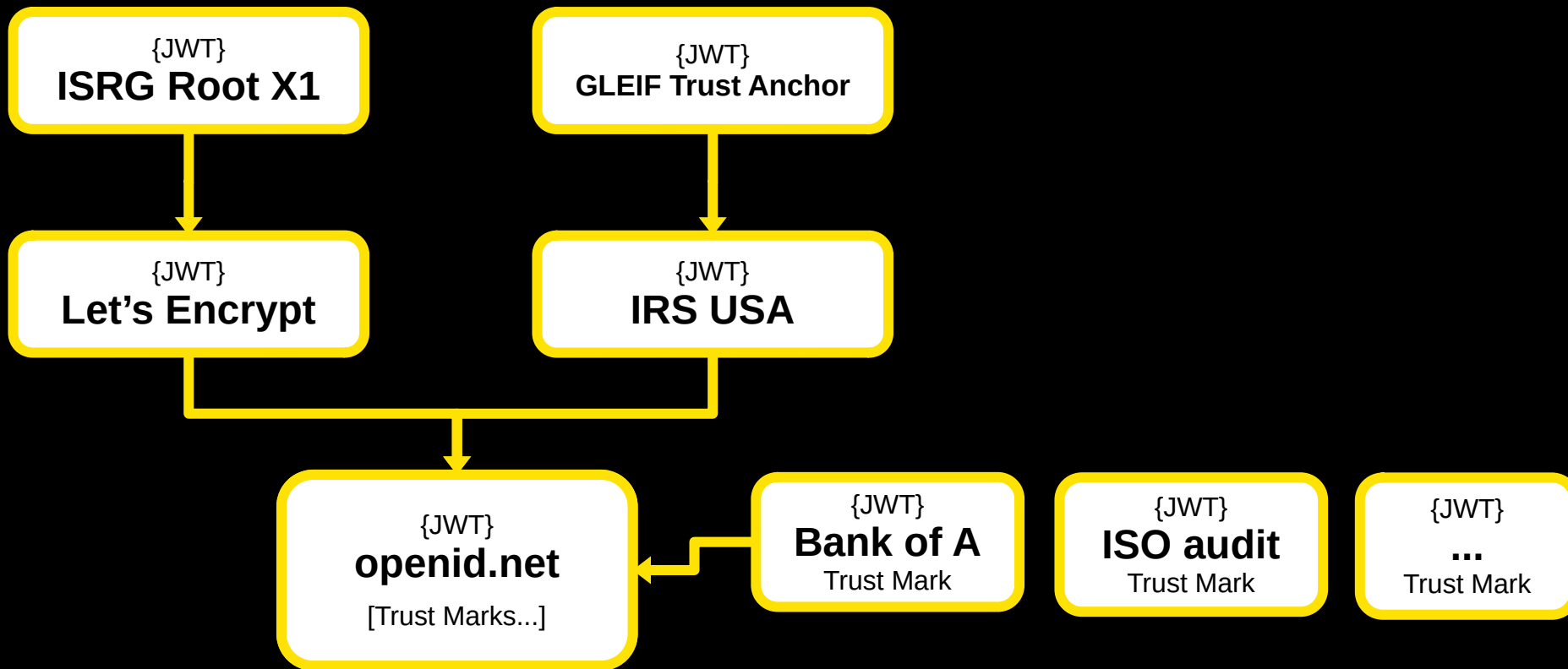
**HOW**  
OpenID Works



# The **Trust Chains** for openid.net

Domain Validation

Legal Entity Validation



# OpenID Federation 1.0 & the Trust Chain

The spec



The story



Questions?



[vd@connect2id.com](mailto:vd@connect2id.com)

[@dzhuvi](#) (X)