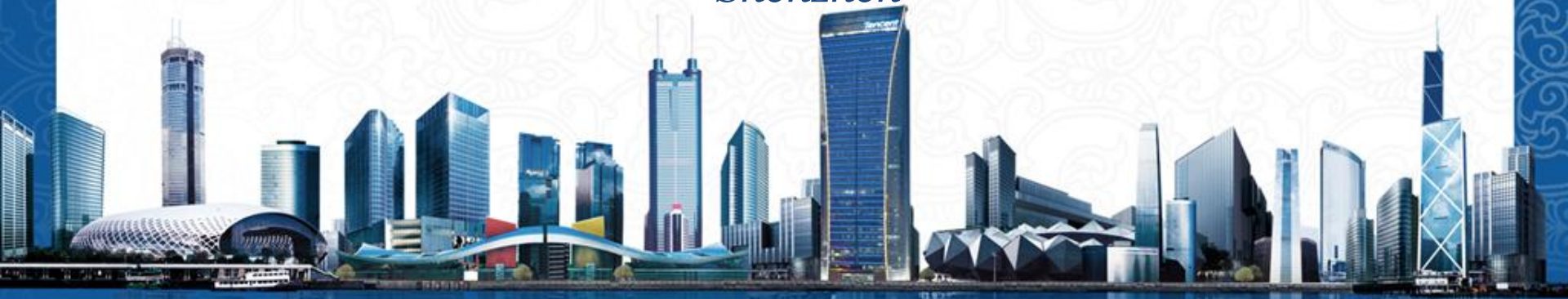
# Security Breakout session #security

*13 November 2013 – W3C TPAC*

*Shenzhen*



# Lets discuss security roadmap in W3C

**Nature of the session**

Two ways discussion : presenting the existing security activity by Wendy & Virginie and gathering your ideas

**Goals**

Collect new use cases, hear what are your security problems, what are your ideal trusted open web platform

**Minimal background**

No special background

# Agenda

- Round table
- W3C current security related security
- What would you like to have more ?
- Wrap-up

# W3C security activity

- The Technology and Society domain
  - Security activity
    http://www.w3.org/Security/Activity
- The WGs
  - XML security WG
  - Web Application Security WG
  - Web Crypto WG
- The Web Security IG
- Open item in TAG

# Problems solved by current activities

**Web App Security** is focusing on making the Single Origin Policy flexible (cross origine for mash up, controlled ressources)

**Web Crypto WG** is delivering an API to build app security model (create credential, generate signature, cipher data …)

**XML Security** allows to handle XML document signature and ciphering from a web (maintenance)

# Few things we know we should do…

- Document the web security model

  Improve the 2002 web security FAQ documentation http://www.w3.org/Security/faq/

  Issue security guidelines/training

  Feed the WebPlatform.org

- Create a security community (again)

  http://lists.w3.org/Archives/Public/public-web-security/

- Include more security features in the open web platform ?

# Which ones ?

Share your security idea, use case, problem, questions…

# Ideas shared by participants

- No binary blob in the browser
- Link trust, peer to peer (see Tim use case)
- Mobile security evidences for the user [more visual indication, warning] which are regressing by the mobile device
- The question is about who controls the web ? Is it service providers (and servers) or user (and client side) → efforts are needed to protect the client side environement or think when it is compromised
- Security researcher and standard relationship need to improve to work on new threat to improve knowledge and be able to correct platform

# Ideas shared by participants

- Use cases and security attacks are large, so how to get focus ? Look at the most scary domains and at the moment the financial services are.
- Certificate chain is broken in browsers, while being a political sensitive topic, it has to be solved.
- Security is large, it is about what I want to control ? Browsers makers are security aware, but we should have the information sharing/captured and educate the user
- Software security/protection is a hard topic (in addition to EME), for example obfuscation is hard on the web → lets harden the software protection

# Ideas shared by participants

- Security should focus on certificate related fonctionalities and security protocol in browser
- Certificate systems is really a pb (TLS MITM attacks), proposals are DNSseconf, key pinning,… Browser vendors have knowledge but do not share.
- Certificate and pki are managed in the browser. It would be good to have the same fluidity on bookmarks and friends management on the crertificates (visible and transparent actions, including the exception management, the self signing scenario, secret question management)
- New use cases : UA in meters/planes/cars are more difficult to secure

# Ideas shared by participants

- XML WG should continue,
- Trust is the goal today we should try to reach, lets actually use the existing tools like HTTPS
- Mathml is not implemented due to security problem, education and sharing is required here
- Security between various applications/parties : how to convene people to identify problems with the user in minds.
- Social networks/website are using a lot cross origin : lets make sure it is secured
- Managed laptops and BYOD have to be solved, to let the user know what is happening to the user's device

# Ideas shared by participants

- Certificate is managed in IETF including key players and it should be a place to talk and share.
- Client certificates and session have to serve the ubiquity scenario → client certificate needs to be linked with a session (reducing the mimtm attacks). Lets make cert server request in web crypto, in sop.
- Functions is layered based (tcp, dns, tls) and the boundaries have to be crossed to have a consistent security → lest have a global vision.
- Use case : identity (see personna) and web payment will be area dealing with security
- Financial services are different in different countries and there are different security levels to be addressed

# Ideas shared by participants

- We have to better know the security model and threat.
  The W3C in europe will publish the security report .

# Directions to move forward

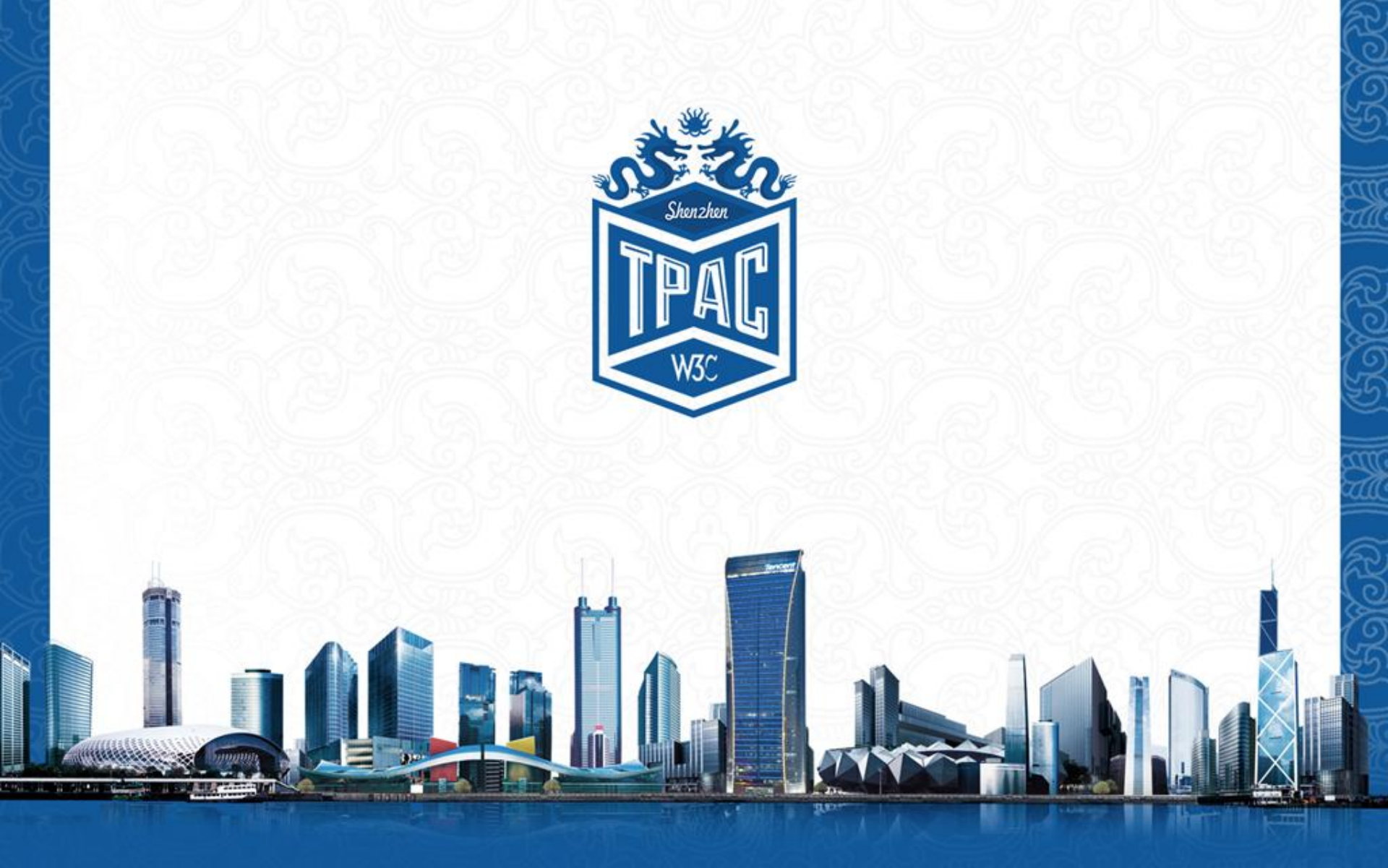
Technology : Thinking of protecting clients side, manage certificate, protect sessions, peer to peer connection

Community: Building standard with more experts, sharing more UA vendor's knowledge

Education : Educate users, educate the W3C community

Contexts: mobile, meters/car/plane…

Domain : payment, social networks environments, identity


Shenzhen
TPAC
W3C