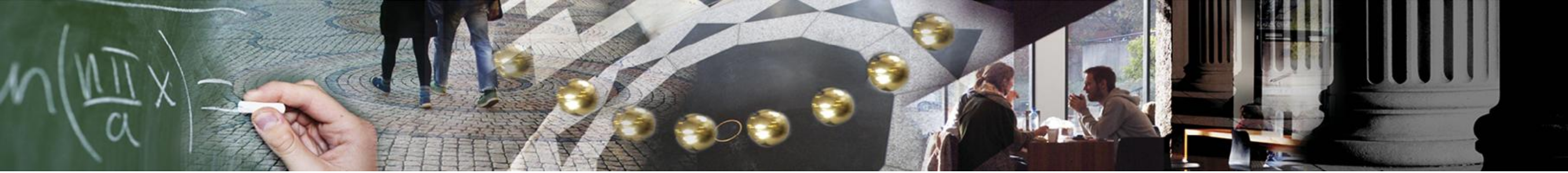


UiO : Department of Informatics
University of Oslo

Enhancing FIDO Transaction Confirmation with Structured Data Formats

Andre Büttner and Nils Gruschka

University of Oslo

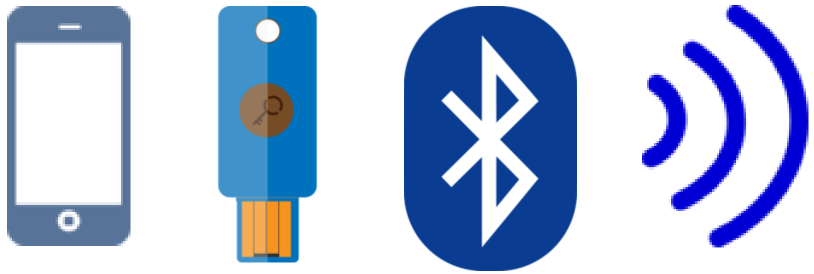
01 December 2021

NIKT 2021 rondheim
29 November – 2 December
Norwegian ICT conference for research and education

Password Authentication

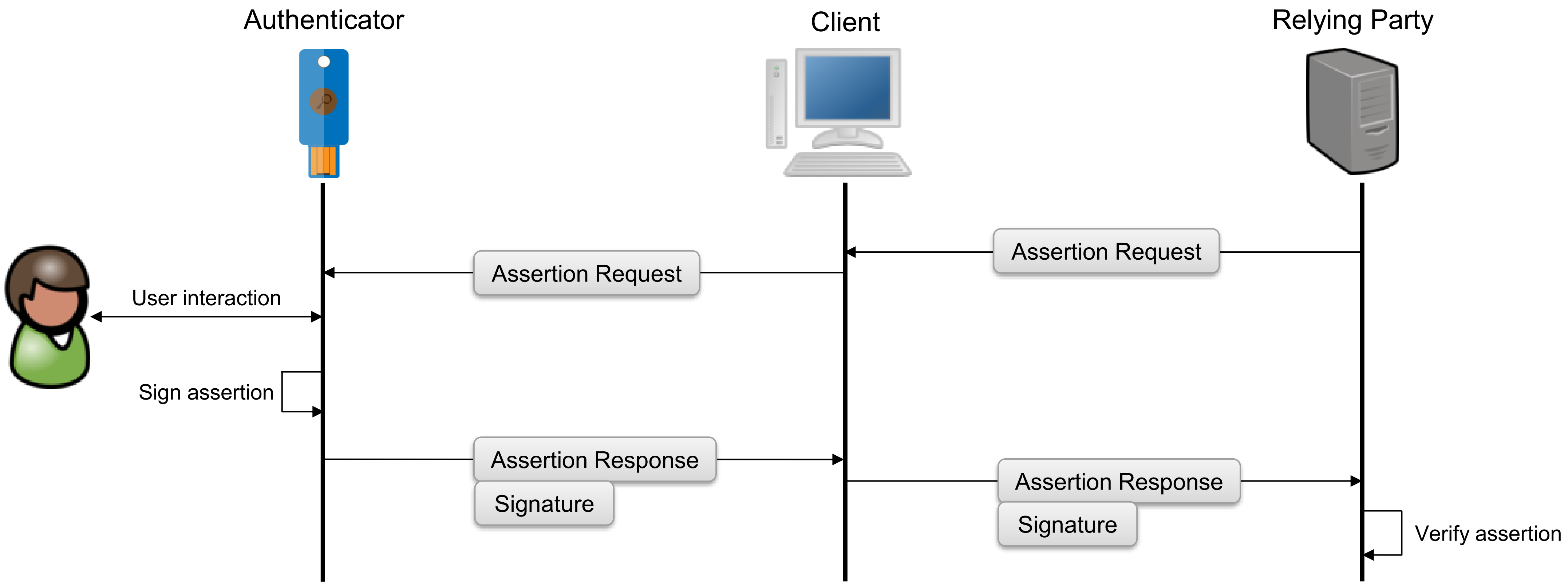
- Something a user **knows**
- Hashed password stored on the server
- Vulnerable to phishing, brute-forcing, etc.
- Often requires additional measures like multi-factor authentication (2FA/MFA) and password managers

FIDO Authentication I



- Something a user **has**
- Additional factor or replacement for passwords
- Roaming/platform authenticators
- Based on public-key cryptography
- The secret never leaves the authenticator
- User presence check by e.g. a button press or biometrics

FIDO Authentication II



FIDO Transaction Confirmation I

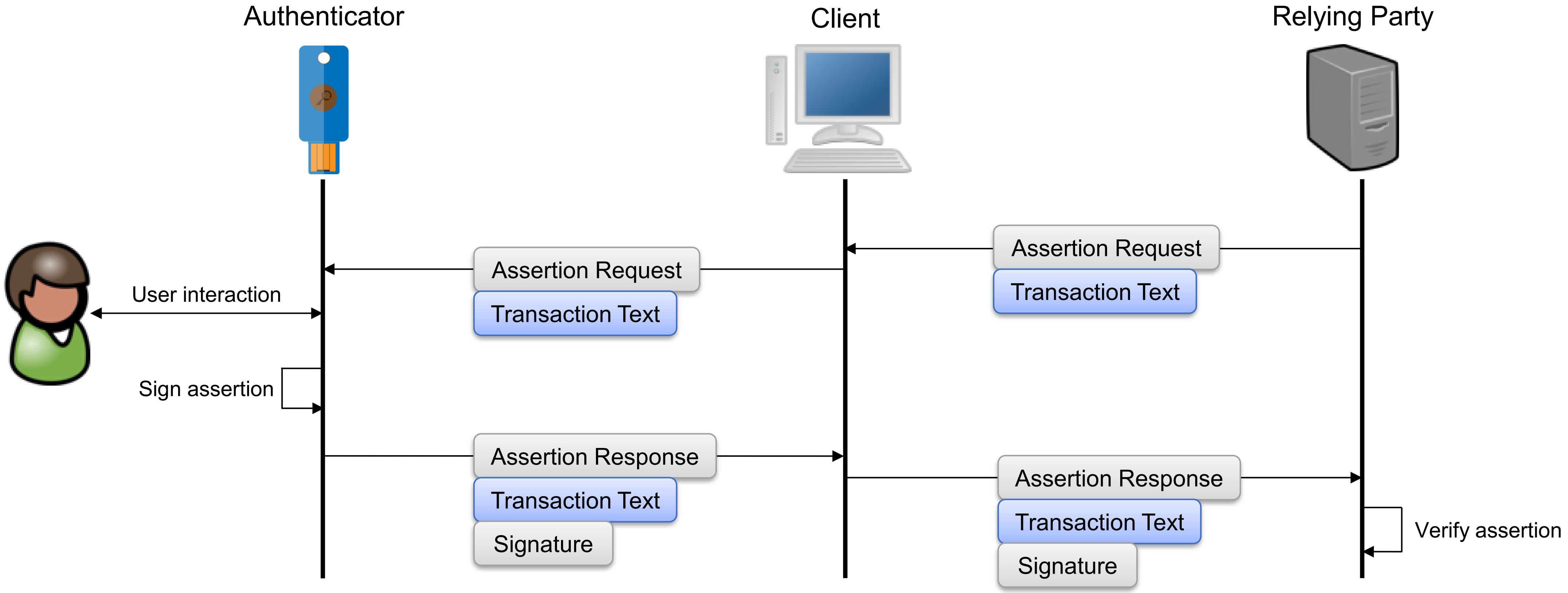
- Proposed in a whitepaper [FIDO Alliance, 2020]
- Protocol extension to include information about a transaction
- Use cases like online banking/purchases or granting access to resources
- Transaction text

```
{
   …
   extensions: {
      txAuthSimple: “Transfer 100.0 NOK to John Doe.”
   }
}
```

- Transaction image

```
{
   …
   extensions: {
      txAuthGeneric: {
         contentType: “image/png”,
         content:     <ArrayBuffer>
      }
   }
}
```

FIDO Transaction Confirmation II



Risks of Transaction Confirmation

- Manipulation by MitM attackers [Zhang *et al.,* 2018], [Xu *et al.*, 2021]
  - E.g. malware or cross-site scripting (XSS)
- User may be tricked into confirming a malicious extension
- No easy way to put constraints to transactions that can be verified automatically
- Ambiguity of transaction text

➔ Violation of What-You-See-Is-What-You-Sign (WYSIWYS) [Landrock and Pedersen, 1998]

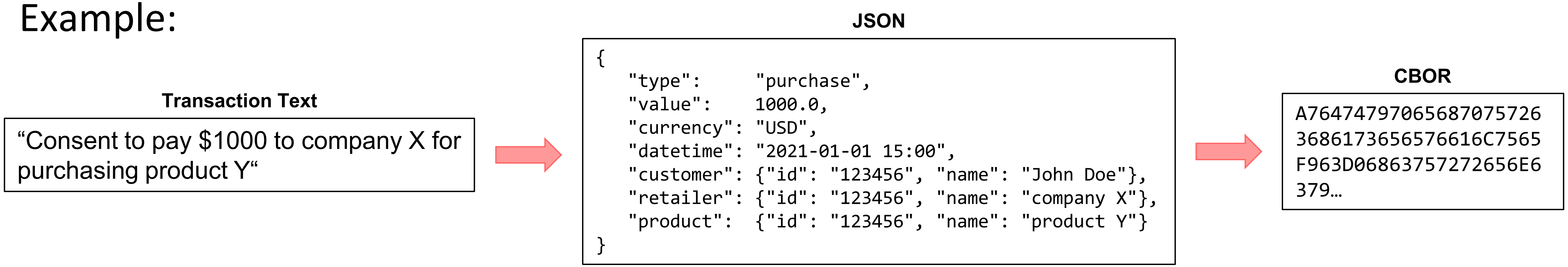
Structured Data for Transactions I

- Self-describing & well-formedness
- Policies can be applied to transaction properties
- XML as common format for (semi-)structured data
    - XML Schema Definition (XSD) language
    - XML Signature and Encryption standards
- FIDO extensions based on
    - JavaScript Object Notation (JSON)
    - Concise Binary Object Representation (CBOR)

```xml
<?xml version = "1.0"?>
<contact>
   <name>John Doe</name>
   <email>john.doe@example.com</email>
</contact>
```

Structured Data for Transactions II

- CBOR
  - Binary data format
  - Particularly useful for low-resource devices such as authenticators
  - Concise Data Definition Language (CDDL)
  - CBOR Object Signing and Encryption (COSE)
- Example:



Transaction Text

“Consent to pay $1000 to company X for purchasing product Y“

JSON

```
{
   "type":     "purchase",
   "value":    1000.0,
   "currency": "USD",
   "datetime": "2021-01-01 15:00",
   "customer": {"id": "123456", "name": "John Doe"},
   "retailer": {"id": "123456", "name": "company X"},
   "product":  {"id": "123456", "name": "product Y"}
}
```

CBOR

```
A76474797065687075726
3686173656576616C7565
F963D06863757272656E6
379…
```

Discussion I

- Formats like XML, JSON or CBOR
  - Can help to avoid ambiguities
  - Can represent more complex types → Filtering of relevant user information
  - Are machine-readable → Applying policies to limit transaction values

- Features like the COSE protocol can prevent manipulation and eavesdropping of extensions

- Definition of schemas
  - By the authenticator → May be difficult on low-resource devices
  - By the client application → Mitigated security gain

Discussion II

- Disadvantages
  - Complexity
  - Increased size of data
  - Latency

Conclusion

- Transaction Confirmation as one of many examples for advanced FIDO use cases
- The proposed extension is too ambiguous and cannot provide WYSIWYS
- Structured formats can facilitate further security measures for FIDO transactions
  - Policies
  - Cryptographic functions

Outlook and Future Work

- Creating test beds for different attack scenarios
- Implementation of transactions using structured data for different FIDO authenticators
- Evaluating CDDL validation and COSE as possible protection measures
- Secure Payment Confirmation [McGruer and Solomakhin, 2021] as replacement for FIDO Transaction Confirmation

References

- FIDO Alliance, ‘White Paper: FIDO Transaction Confirmation’, Aug. 21, 2020. https://fidoalliance.org/white-paper-fido-transaction-confirmation/
- Y. Zhang, X. Wang, Z. Zhao, and H. Li, ‘Secure Display for FIDO Transaction Confirmation’, in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, New York, NY, USA, Mar. 2018, pp. 155–157. doi: 10.1145/3176258.3176946.
- P. Xu, R. Sun, W. Wang, T. Chen, Y. Zheng, and H. Jin, ‘SDD: A trusted display of FIDO2 transaction confirmation without trusted execution environment’, *Future Generation Computer Systems*, vol. 125, pp. 32–40, Dec. 2021, doi: 10.1016/j.future.2021.06.034.
- P. Landrock and T. Pedersen, ‘WYSIWYS? — What you see is what you sign?’, *Information Security Technical Report*, vol. 3, no. 2, pp. 55–61, Jan. 1998, doi: 10.1016/S0167-4048(98)80005-8.
- Stephen McGruer and Rouslan Solomakhin. ‘Secure Payment Confirmation’, W3C Working Draft, Aug. 31, 2021. https://www.w3.org/TR/2021/WD-secure-payment-confirmation-20210831/

Thank you!