IFC Implementers Forum

General Assembly of Implementers

Westminster (CO) USA

28th August 2024

Wed 28 August	Time (MDT)	Duration (mins)	Topic	Speaker(s)
Session 1: IDS, IFC, bSDD	09:00 - 10:30	15	**Welcome and introduction from Trimble & buildingSMART**	Chris Cronin, Ian Howell
		30	**Status update of standards and services**	Léon van Berlo
		45	**User experiences and feedback**	Richard Brice
	11:00 - 12:30	15	**IDS updates & Software Certification**	Artur Tomczak
		60	**bSDD updates**	Artur Tomczak
		15	**IFC 4.3 & Implementer Forum update**	Evandro Alfieri
Lunch	12:30 - 13:30		**Lunch & Group Photo**	
Session 2: IFC Validation & Certification	13:30 - 15:00	90	**IFC Validation Service**	Evandro / Scott Lecher
	15:30 - 17:00	60	**IFC Software Certification**	Evandro / Léon
		30	**IFC Geometry tiger team**	Angel?
	17:30		**Dinner hosted by Trimble - Kachina Southwestern Grill**	

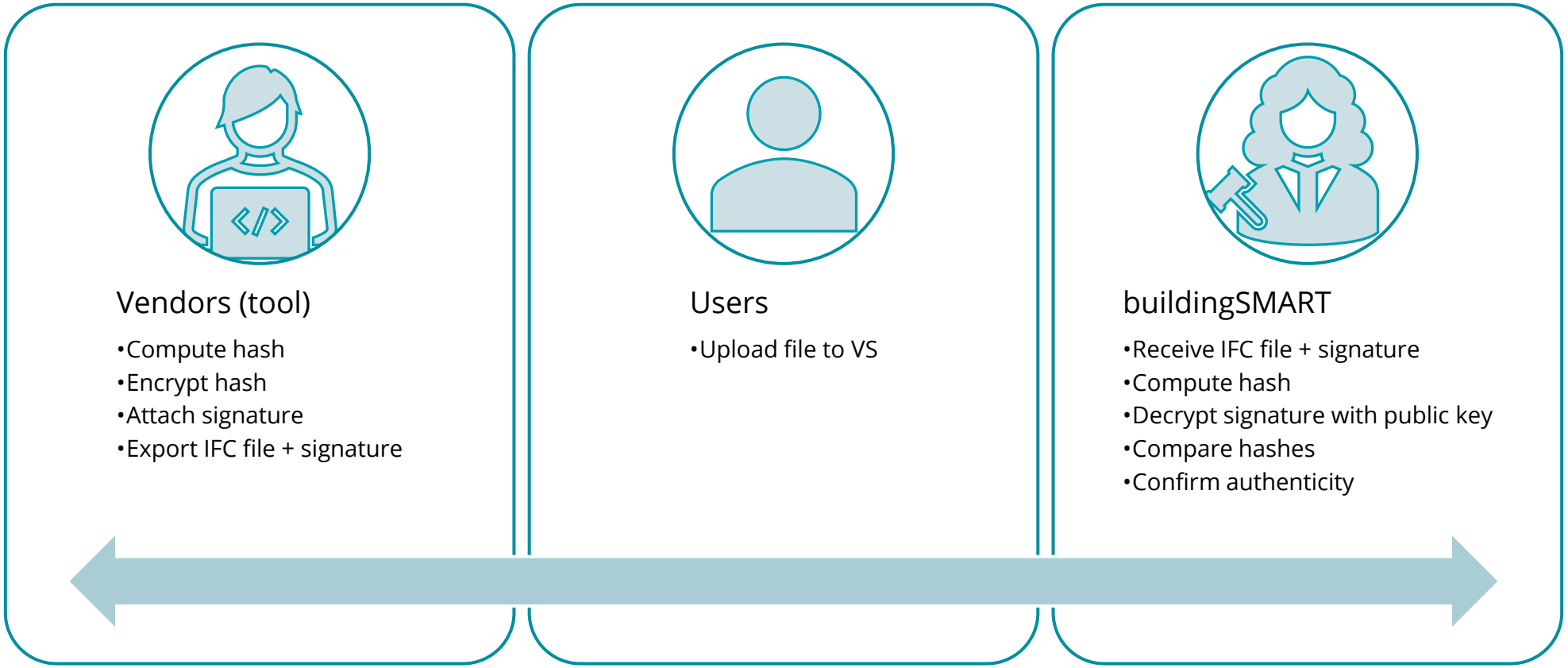
Content

- Integrity and authenticity of IFC using digital signature

Goal

Ensure the **integrity** and **authenticity** of **IFC files** and verify that they have **not been tampered with** or **altered after being produced** by specific software tools

Workflow (simplified, but not much)



Agreements

Key Management

- **Key Generation:** Vendors must generate their own public-private key pairs.
- **Public Key Distribution:** Suggest a method for Vendors to share their public keys with buildingSMART.
- **Key Storage:** Vendors must securely store their private keys and buildingSMART must securely store the public keys.

Agreements

Signature Creation and Attachment

- **Hash Algorithm:** Agree on a standard cryptographic hash algorithm (e.g., SHA-256) to be used for generating the hash of the IFC files.
- **Signature Algorithm:** Agree on a standard encryption algorithm (e.g., RSA) to be used for encrypting the hash.
- **Signature Storage:** Define a standardized way to store the digital signature.
  - Embedding the signature as metadata within the IFC file.

(no) Agreements

Verification Process

- **Hash Computation:** buildingSMART will compute the hash of the received IFC file using the agreed-upon hash algorithm.
- **Signature Decryption:** buildingSMART will decrypt the digital signature using the vendor's public key.
- **Hash Comparison:** buildingSMART will compare the computed hash with the decrypted hash to verify the file's integrity.

Agreements

Communication and Support

- **Documentation:** Provide clear documentation and guidelines for vendors on how to generate and attach digital signatures.
- **Support:** Establish a support channel for vendors to assist with any issues related to the digital signature process. Email?
- **Regular Updates:** Agree on a protocol for regular updates and communications regarding any changes in the process or algorithms used.

Agreements

Testing

- **Pilot Testing:** Agree on a few vendors to conduct pilot testing, to ensure the process works smoothly before full-scale implementation.

Action plan

1. **Initiate Discussions:** (today)
2. **Draft Agreements:** Draft formal agreements covering the key points listed in previous slides.
3. **Develop Documentation:** Create documentation and guidelines for the vendors.
4. **Key Distribution Mechanism:** Set up a mechanism for public key distribution.
5. **Pilot Program:** Launch a pilot program with selected vendors to test the process.
6. **Full Implementation:** Roll out the process to all vendors after successful pilot testing.
7. **Monitor and Support:** Continuously monitor the implementation and provide support as needed.

Questions