

Digital Image Integrity

Derek Davis

Data Security Component Architect

Intel Corporation

(602) 554 8348

Derek_L_Davis@ccm.ch.intel.com

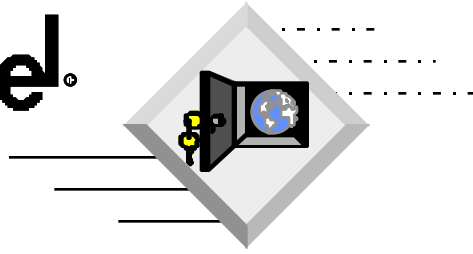
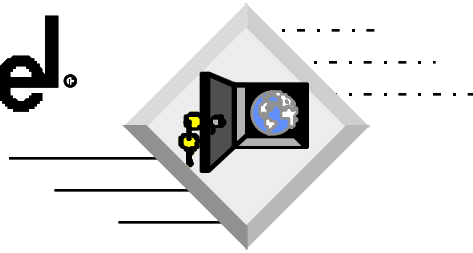


Image Integrity - what's the issue?

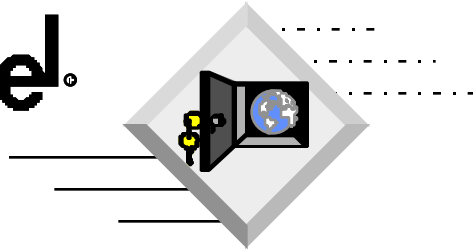
- **We used to “trust” photographs and videos**
- **That “trust” has already been significantly reduced in the print domain**
 - availability of morphing capability for “professional” use
 - willingness of publishers to use such capabilities to questionable purpose



Transitioning Domains Print/Broadcast to Electronic

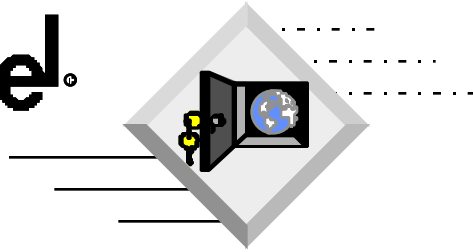
- **No longer even have physical instantiation as a source of trust**
- **Decreasing cost of morphing capability means wide-spread accessibility**
- **Results in further degradation of trust-basis in electronic images**

⇒ Need to reestablish a trust-basis for images



Aspects of Image Integrity

- **Authenticity of capture** **HOW**
- **Time of capture** **WHEN**
- **Location of capture** **WHERE**

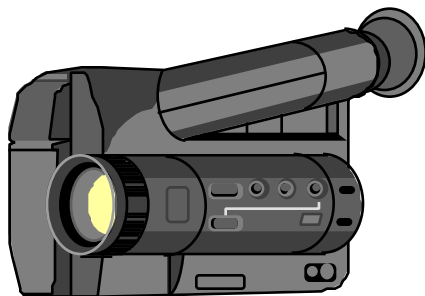


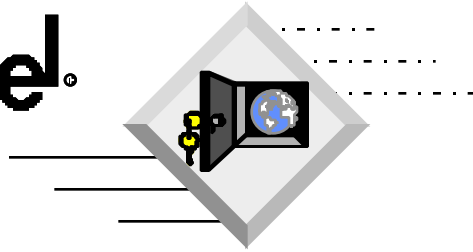
Authenticity of Captured Image

Signaturing Digital Camera

- Camera's private key used to digitally-sign captured still image or video clip
- Hardware-embedded, manufacturer-certified key-pair

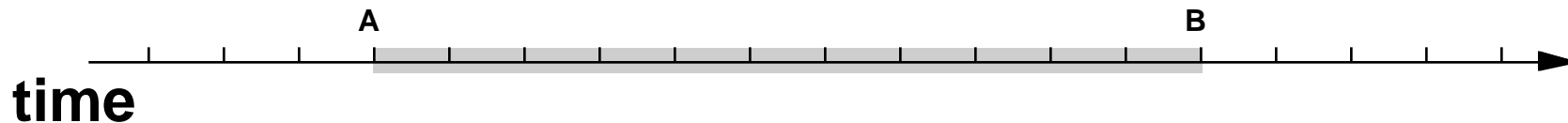
⇒ Image signature with device certificate prevents undetectable image morphing

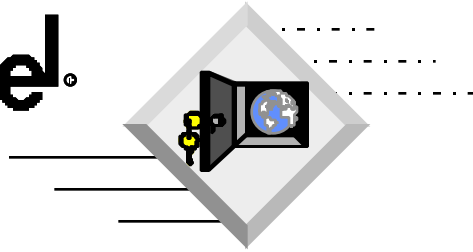




Time of Capture

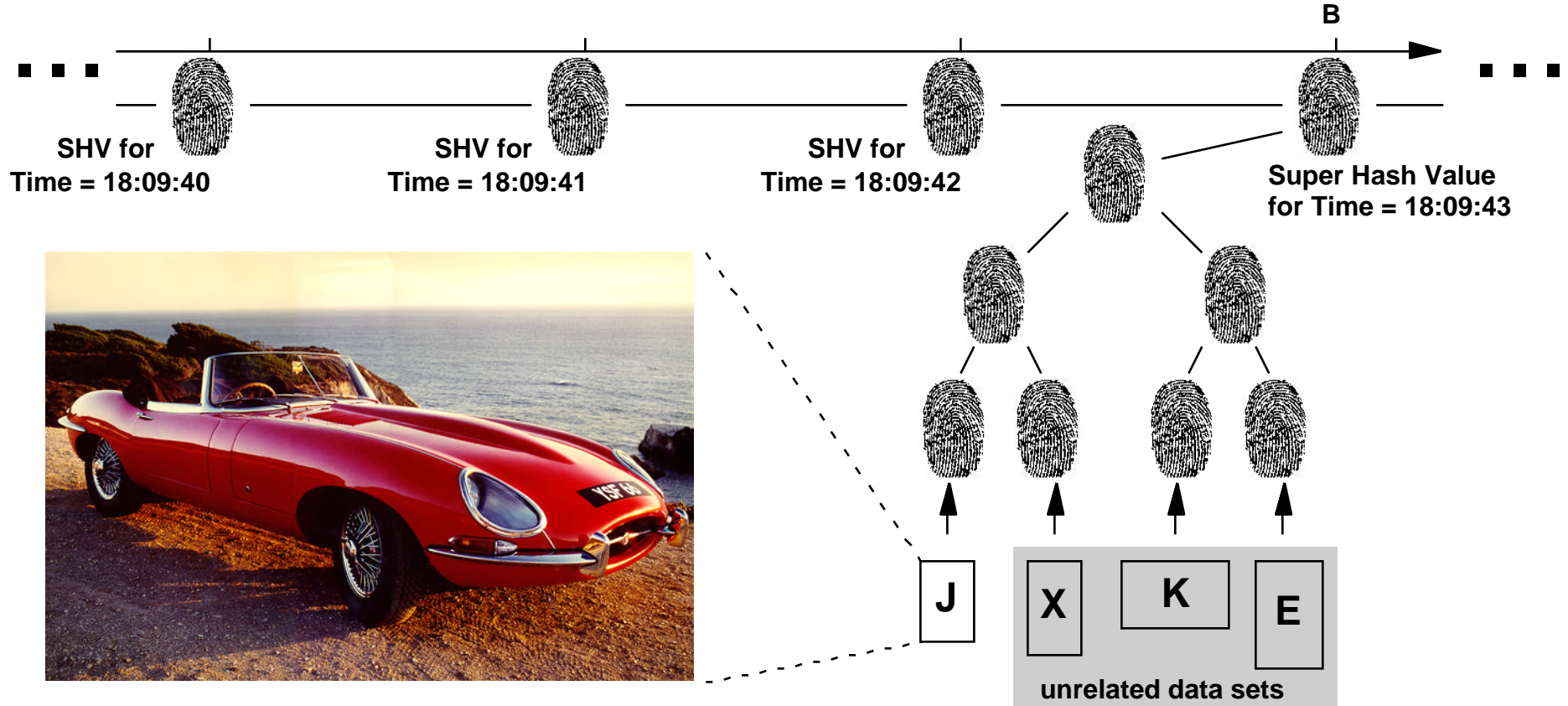
- **Time of Capture is problematic**
 - implies trusted real-time clock source
 - issues with initialization, natural drift, induced drift, etc.
- **“Timeframe of Capture” means**
 - captured after timepoint “A” and
 - captured before timepoint “B”

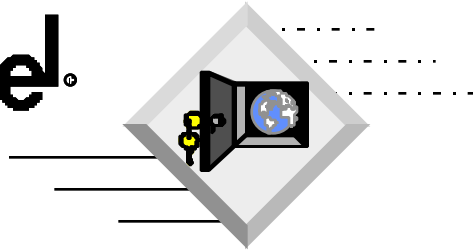




Demonstrating Capture Before Timepoint “B”

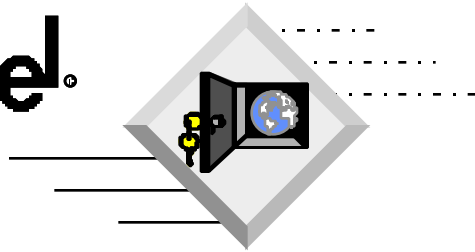
- Prevents after-the-fact tampering, scene creation
- Addressed by Haber/Stornetta with hash trees





Demonstrating Capture After Timepoint “A”

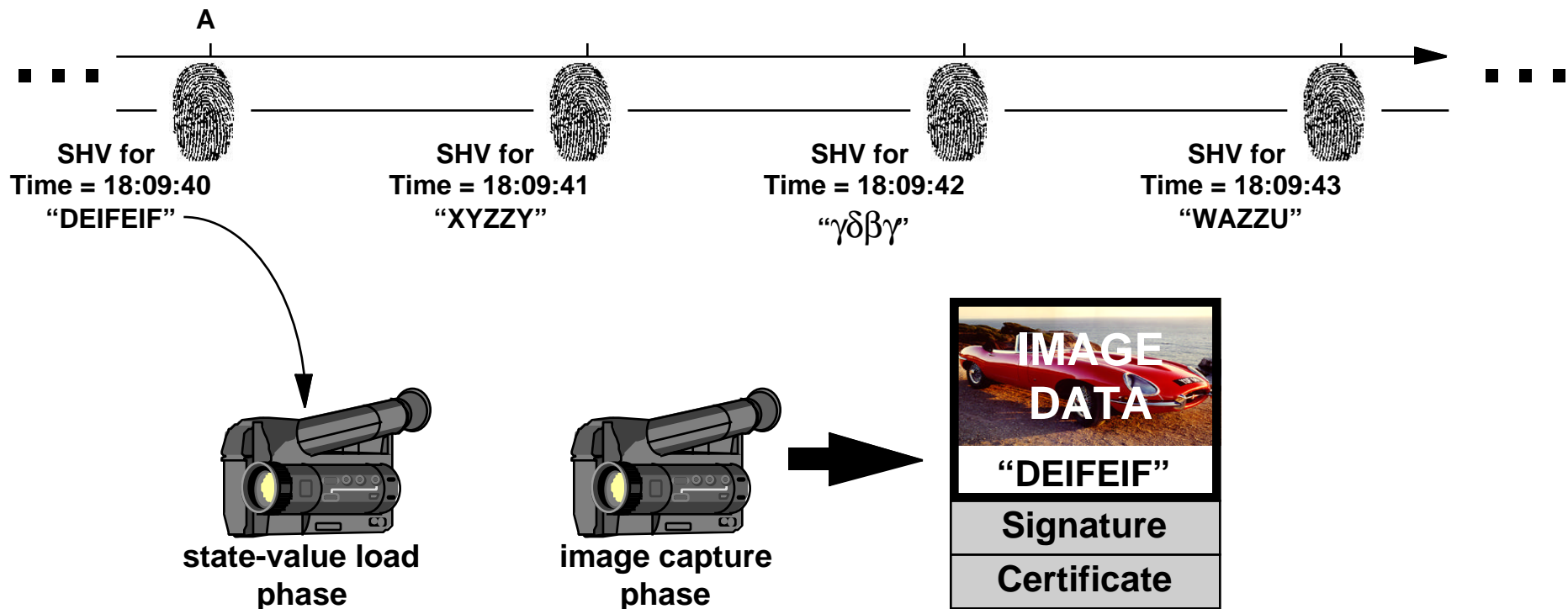
- **Prevents before-the-fact scene creation**
 - insurance claims
 - kidnapping
- **Addressed with extension of techniques discussed**
 - hash-based time-stamping to provide relative time reference
 - trusted functionality of the image capture device
 - image signature with device certificate

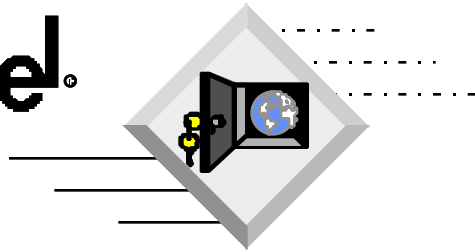


Use of State Value to Establish Timepoint “A”

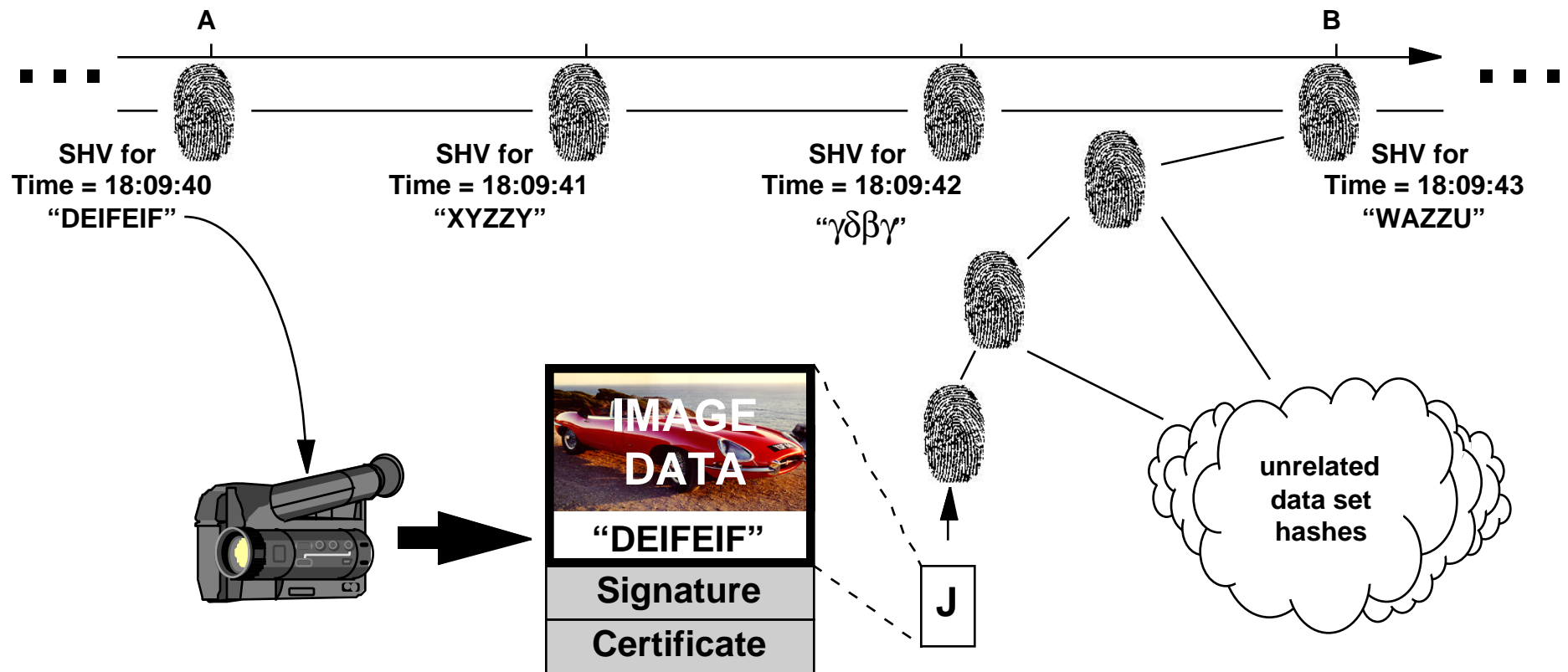
Atomic Operation

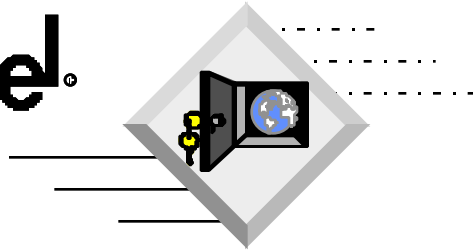
- State-value is loaded prior to image capture
- Image data includes state-value, image is signed





Time Bracketing Realized

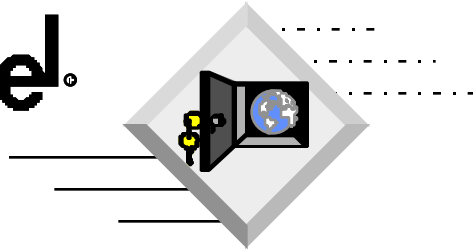




Integrity Validation

Three Validations

- **How?**
 - Read Device Certificate using widely-known Manufacturer Public Key
 - Validate Image Signature using Device Public Key
- **When?**
 - Derive “Time A” from State-Value in the signed image
 - Derive “Time B” from the hash-based time-stamp information



Conclusion

- **Use of these techniques can provide a degree of “trust” in images in the electronic domain**
- **Raises the bar for fraudulent creation and use of digital images**
- **Allows photographers/publishers to regain the “high ground” of integrity lost to morphing capability**
- **While not preventing physical scene creation, these techniques constrain it to have occurred coterminally with claimed event**