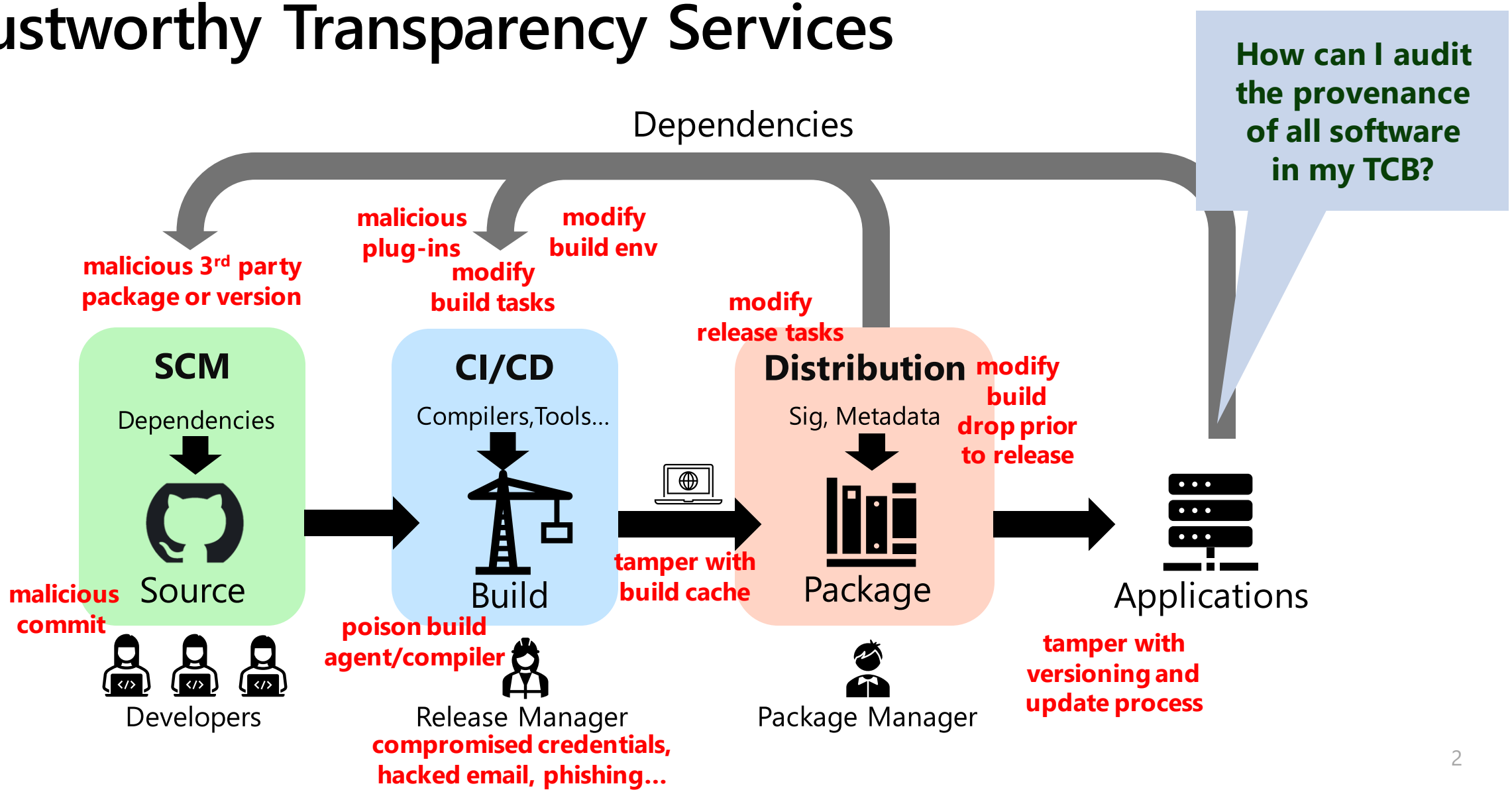
Trustworthy Digital Supply Chain Transparency Services

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>
on behalf of SCITT contributors (W. Bartholomew, H. Birkholz, S. Clebsch, A. Deligat-Lavaud, Y. Deshpande, C. Fournet, B. Knight, S. Lasker, S. Provine, M. Riechert, A. Stewart, K. Williams, R. Williams, … see scitt@ietf.org)

https://www.ietf.org/archive/id/draft-birkholz-scitt-architecture-00.html
https://www.ietf.org/archive/id/draft-birkholz-scitt-receipts-00.html

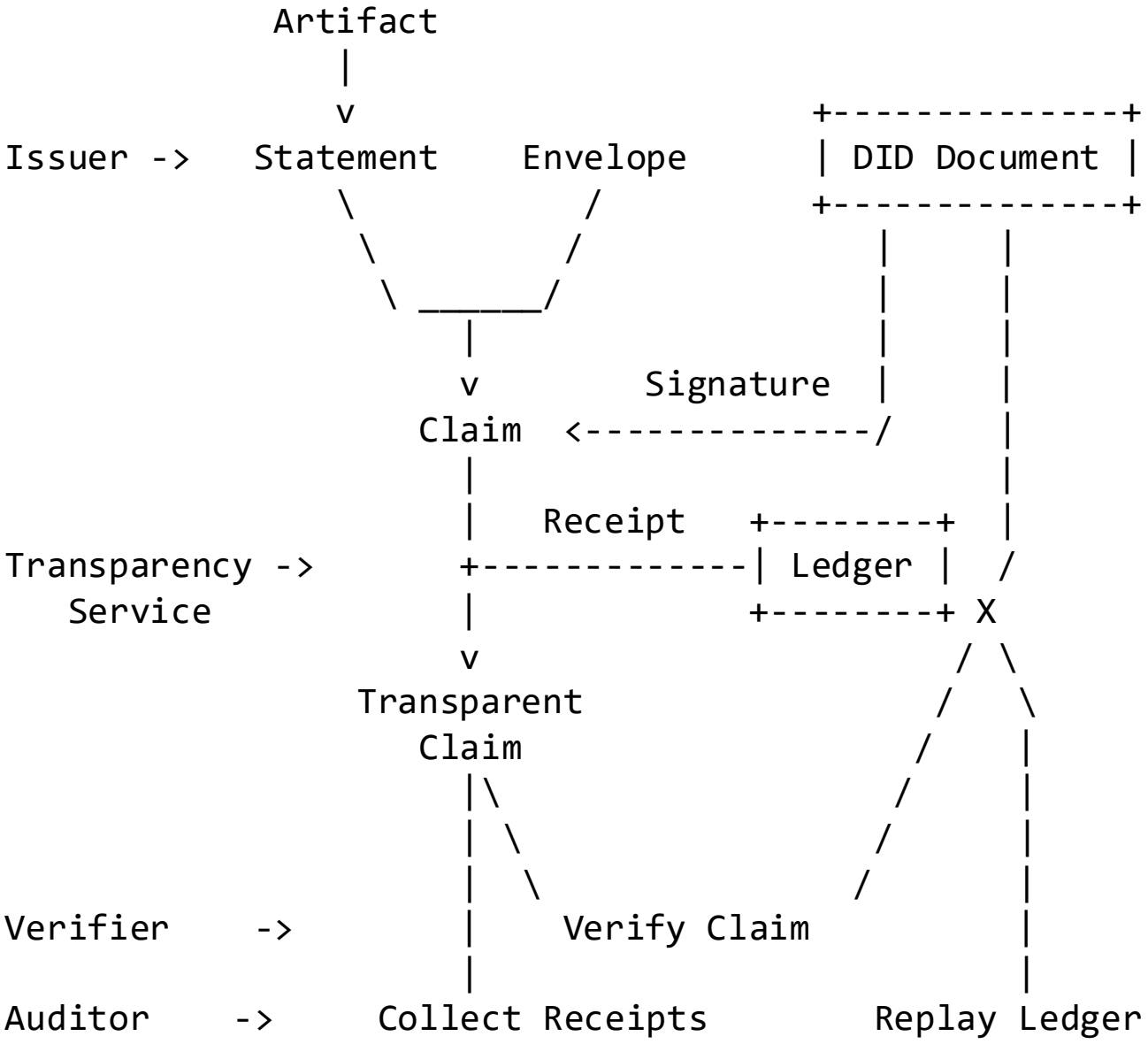
HoTRFC @ IETF 113, Sun March 19th, 2022

Countering Software Supply Chains Attacks: Trustworthy Transparency Services



SCITT Architecture and Receipts

```
SCITT_Receipt = {
; Hash of transparency service key
    "serviceId"     => bstr
; Transaction id
    "transactionId" => tstr
; Signature algorithm
    "alg" => int
; Signature over tree root
    "signature" => bstr
; Intermediate hashes (Merkle path)
    "proof" => [+ ProofElement]
}
```



Related Work and Working Groups in the IETF

- Envelopes & Receipts are based on COSE WG output
- Transparency service operations trustworthiness involves RATS WG output
- Transparency services borrow concepts and terms from the concept of Certificate Transparency defined in RFC 6962