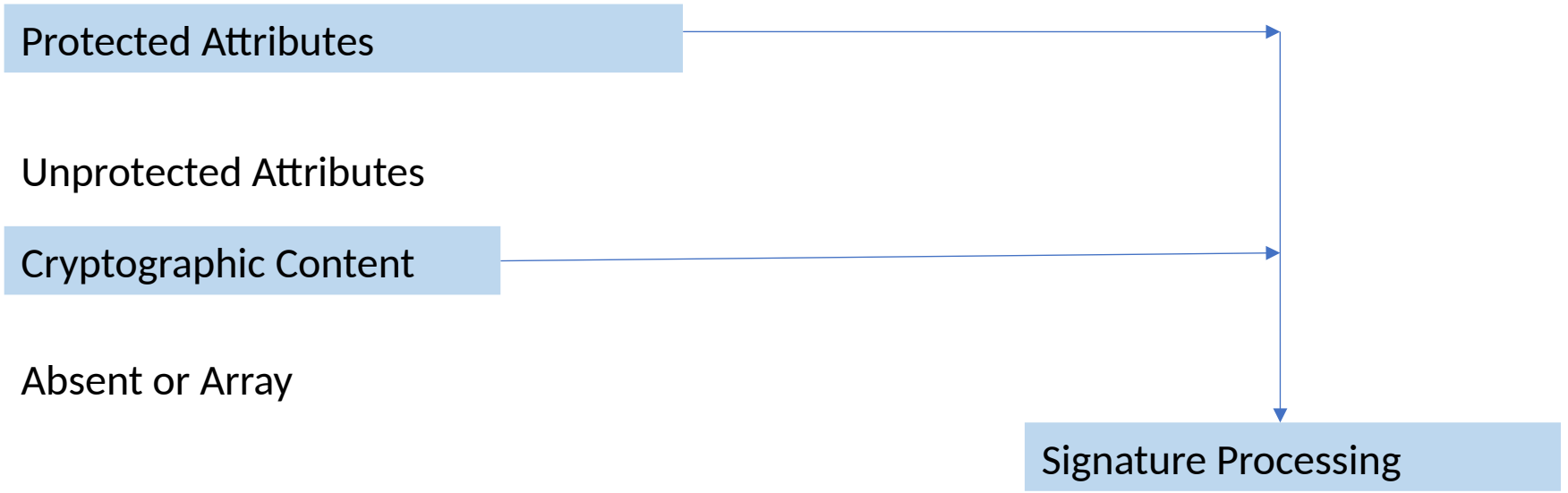
COSE: Structure Discuss

Jim Schaad

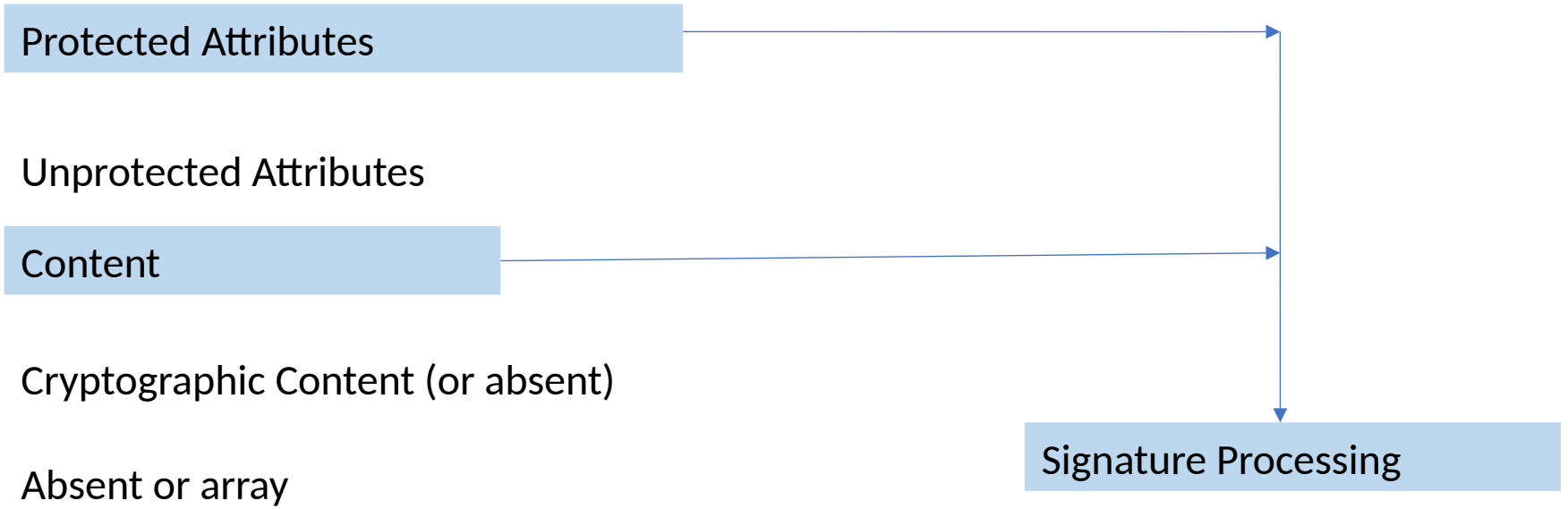
August Cellars

Get a “real” countersignature



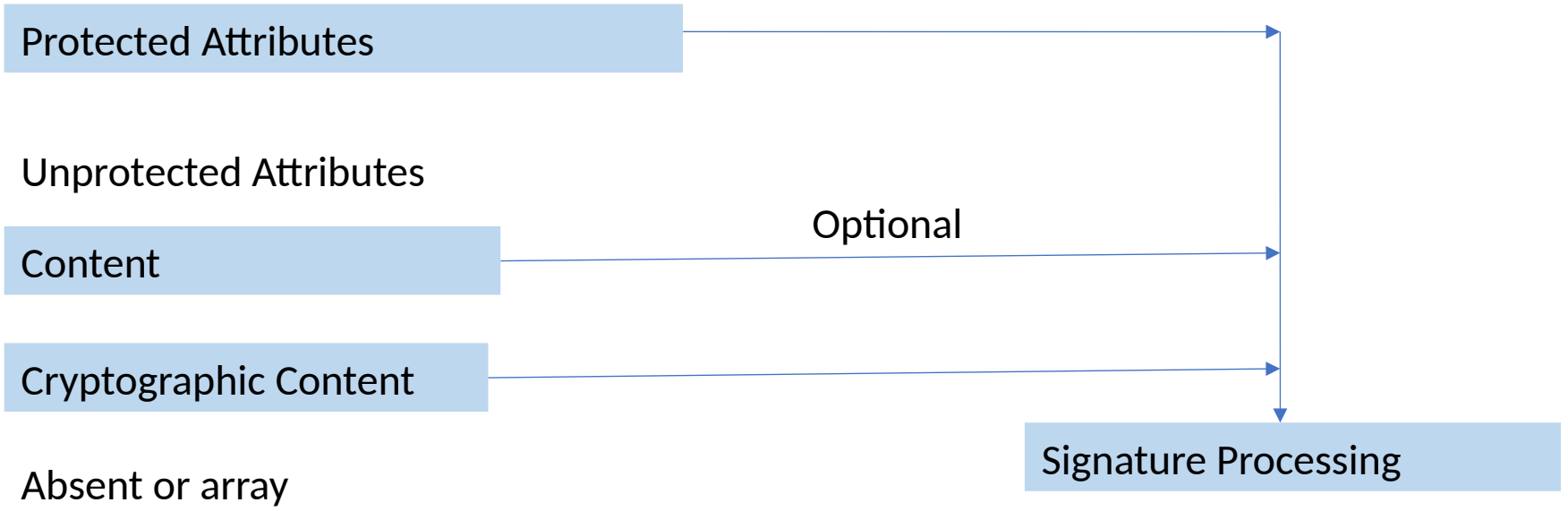
- Content is cryptographic value for COSE_Encrypt*, COSE_Recipient and COSE_Signer

Just Generate a parallel signature



- Content is NOT cryptographic value for COSE_MAC*, COSE_Signature, COSE_Sign0

Change the Countersignature Algorithm



- Include <first, last> bstr or include <all> bstr

Which way is the document altered?

- HUM: Leave things along and you cannot countersign COSE_Sign0
- HUM: Fix it so countersign COSE_Sign0 works correctly

- If hum says fix things then

- HUM: Be aggressive on what is signed – all bstr elements
- HUM: Be constrained on what is signed – first and last bstr element