Assignment 6 (practice only): Problems on Trusting Trust
15-316 Software Foundations of Security and Privacy

1. **Unfinished business.** Finish the proof of $\Gamma \vdash \mathsf{mfredrik}\ \mathtt{says}\ \mathtt{read}(\text{'15316-grades.xlsx'})$ from the following assumptions.

$$
\begin{aligned}
Q_1 &\equiv \mathtt{isKey}(\mathsf{ca}, \mathsf{pk}_{\mathsf{ca}}) \\
Q_2 &\equiv \mathtt{sign}_{\mathsf{sk}_{\mathsf{ca}}}(\mathtt{isKey}(\mathsf{tpm}, \mathsf{pk}_{\mathsf{tpm}})) \\
Q_3 &\equiv \mathtt{sign}_{\mathsf{sk}_{\mathsf{tpm}}}(\mathtt{isKey}(\mathsf{os}, \mathsf{pk}_{\mathsf{os}})) \\
Q_4 &\equiv \mathtt{sign}_{\mathsf{sk}_{\mathsf{mfredrik}}}(\forall x.(\mathsf{os}\ \mathtt{says}\ \mathtt{read}(x)) \rightarrow (\mathsf{mfredrik}\ \mathtt{says}\ \mathtt{read}(x))) \\
Q_5 &\equiv \mathtt{sign}_{\mathsf{sk}_{\mathsf{os}}}(\mathtt{read}(\text{'15316-grades.xlsx'})) \\
Q_6 &\equiv \forall x.(\mathsf{tpm}\ \mathtt{says}\ \mathtt{isKey}(x, \mathsf{pk}_x)) \rightarrow \mathtt{isKey}(x, \mathsf{pk}_x) \\
Q_7 &\equiv \mathtt{isCA}(\mathsf{ca})
\end{aligned}
$$

   Note: The lecture notes did not mention the assumption $\mathtt{isKey}(\mathsf{mfredrik}, \mathsf{pk}_{\mathsf{mfredrik}})$*, which you can use in your assumptions and denote* Q_8*.*

2. **Countersigning.** It is common practice in PKI to have the CA issue weaker certificates that rely on a *countersignature* for verification. So suppose that ca is the certificate authority and cs is the countersigner. Then ca might issue a certificate to cmu that consists of the following.

$$\mathtt{sign}_{\mathsf{sk}_{\mathsf{ca}}}(\mathsf{cs}\ \mathtt{says}\ \mathtt{isKey}(\mathsf{cmu}, \mathsf{pk}_{\mathsf{cmu}}) \rightarrow \mathtt{isKey}(\mathsf{cmu}, \mathsf{pk}_{\mathsf{cmu}})) \tag{1}$$

   Then cs must issue a second certificate, which comes with an expiration date.

$$\mathtt{sign}_{\mathsf{sk}_{\mathsf{cs}}}(\mathtt{isbefore}(\mathit{exp}) \rightarrow \mathtt{isKey}(\mathsf{cmu}, \mathsf{pk}_{\mathsf{cmu}})) \tag{2}$$

   Part 1. Explain how one can verify the authenticity of $\mathsf{pk}_{\mathsf{cmu}}$ from (1) and (2), along with assumptions $\Gamma = \mathtt{isCA}(\mathsf{ca})$, $\mathtt{isKey}(\mathsf{cs}, \mathsf{pk}_{\mathsf{cs}})$, $\mathtt{isbefore}(\mathit{exp})$.

   Part 2. Explain how countersigning can mitigate the effects of key compromise. In particular, describe the consequences of cmu's private key being compromised if the corresponding public key is certified in this way, and how they are less severe than if cmu had obtained a certificate directly from ca. Then describe the consequences of cs's signing key being compromised, and why this is less severe than if ca's signing key is compromised.