Assignment 5: Authorization & Trust
15-316 Software Foundations of Security and Privacy

1. *A* **speaks for** *B* **(25 points).** Suppose that $\mathsf{mfredrik}$ wishes to *delegate* his authority to claim students using $\mathtt{studentOf}(x, \mathsf{mfredrik})$ to bcook, so that statements of the form $\mathsf{bcook}\ \mathtt{says}\ \mathtt{studentOf}(x, \mathsf{mfredrik})$ are treated the same as statements of the form $\mathsf{mfredrik}\ \mathtt{says}\ \mathtt{studentOf}(x, \mathsf{mfredrik})$.

   - **Part 1 (5 points).** Write an authorization logic policy formula Q_d that accomplishes this.
   - **Part 2 (10 points).** Use your policy from Part 1, in addition to the formula wherein bcook says that urvia is a student of $\mathsf{mfredrik}$, i.e. $Q_b \equiv \mathsf{bcook}\ \mathtt{says}\ \mathtt{studentOf}(\mathsf{urvia}, \mathsf{mfredrik})$, to prove the judgement below.

   $$Q_d, Q_b \vdash \mathsf{mfredrik}\ \mathtt{says}\ \mathtt{studentOf}(\mathsf{urvia}, \mathsf{mfredrik})$$

2. **Countersignatures (25 points).** 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, and cmu wants a key signed. One way to accomplish this might be to have ca issue a certificate to cmu that consists of the following.

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

Then cs must issue a second certificate, which comes with an expiration date for a particular key $\mathtt{pk}_{\mathsf{cmu}}$, modeled by $\mathtt{isbefore}(exp)$, where exp is the expiration date of the countersignature.

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

Note that rather than signing a public key unconditionally, the ca signs the public key conditional on a statement from the countersigner that the key is still valid. This can partially mitigate the consequences of leaked keys, because the countersignature can have a short expiration period, so after a countersigned key is leaked, the vulnerable party simply lets the countersignature expire.

(a) **(10 points).** Demonstrate how a remote party can use *(1)* and *(2)*, along with knowledge of the ca's public key and cs's public key, to establish $\mathtt{isKey}(\mathsf{cmu}, \mathtt{pk}_{\mathsf{cmu}})$. Your answer can either be a formal proof, or a natural-lanauge description of the steps, including the relevant proof rules, that the remote party should take to establish $\mathtt{isKey}(\mathsf{cmu}, \mathtt{pk}_{\mathsf{cmu}})$.

(b) **(15 points).** If cs is compromised, then this approach is vulnerable. Assuming that an attacker mal has access to cs's secret key $\texttt{sk}_{\mathsf{cs}}$, describe what they must do to convince someone that their public key belongs to cmu, i.e. $\texttt{isKey}(\mathsf{cmu}, \texttt{pk}_{\mathsf{mal}},)$. Then, explain how to remove this vulnerability by making changes to either *(1)* or *(2)* (or both).