SIL765: Network & System Security: projects

Listed below, you will find brief description of 6 projects, numbered 0 through 5. In groups of 2, you are required to pick one (see algorithm to pick a project), complete that project and submit a report (with a working system) on or before March 13. The outcome will be evaluated by me.

Algorithm to pick a project: you are required to pick project numbered 0, 1, 2, 3, 4 or 5 as determined by
k = A1+A2 mod 6, where
A1 = last_4_digits_of_entry_no_of_first_student, and
A2 = last_4_digits_of_entry_no_of_second_student.

The submission will consist of three parts:

1. a 2 to 4 page document describing the system you have designed,
2. the code as a separate file, and
3. 5 to 8 slides that you will use to present your work.

Project 0:
This application relates to keeping and providing a certified copy of the current time and date in a secure manner. In particular a client should be able to request and obtain a digitally signed copy of the current GMT data and time. There are two ways to do this.

1. access a web based "GMT data and time server" which then returns a file which contains the current GMT data and time, suitably signed digitally with the server's RSA-based private key, OR
2. send a mail to a server which "immediately" returns a file which contains the current GMT data and time, suitably signed digitally with the server's RSA-based private key.

Further:

1. Use the date/time so obtained to set the time on your mobile or the laptop.
2. And, ensure that the date/time server itself gets the correct, and certified, GMT time and date from a reliable source (Question: what is a reliable source?).
3. Also ensure that the client has the correct "public-key" of the date/time server and uses that to verify authenticity, integrity of the message containing the data/time.
4. Would access to "public-key certificate" issued by a certification authority be an issue?

Project 1: This application relates to time-stamping a document that one may have prepared some moments ago, and returning it in a secure manner with the date/time appended to it. Assuming that the "GMT date and time-stamping server" has the correct GMT date and time, it time-stamps the document (in some standard format) with the current GMT data/time and a digital signature. At any time, it should be possible to establish the fact that the document existed at the date/time stamped, and that the document has not been modified.
Further:

1. How do you ensure privacy, in that the server does not see/have/keep the original document?
2. How do you share the document with others in a secure manner with the date/time preserved, and integrity un-disturbed?
3. Also ensure that the user has (and uses) the correct "public-key" of the date/time stamping server.
4. Would access to "public-key certificate" issued by a certification authority be an issue?

Project 2: This application relates to building a web server that responds with a degree-certificate and grade-card whenever someone requests for it. The request must contain the graduate's unique entry-

number. The degree-certificate and grade-card (possibly in PDF format) are suitably digitally signed by the university authorities.

1. How do you get the document to be signed by more than one individual (say two persons)?
2. How do you ensure that only the graduate is able to download it (by providing information beyond the entry_no, such as date of birth, home pin code, etc.?
3. Should the graduate decide to share the document with others, how can one trace the origin of the document (could watermarks be useful?)?
4. Would access to "public-key certificate" issued by a certification authority be an issue?

Project 3: The origin of this lies in UID project of GoI, where a central server can be accessed to determine whether some information on an individual is correct or not, but without divulging the information itself. For instance, the database will help determine whether BNJ's DoB is xxx or not, but without the database server itself volunteering such information. How can we do this in a secure and trusted manner.

1. One question that arises is: how does one ensure that information is not altered during the 2-way communication between the client and server?
2. How could one be sure that the reply from UID server "Yes" or "No" is related to the question being asked?
3. In what way are digital signatures relevant?
4. Would access to "public-key certificate" issued by a certification authority be an issue?

Project 4: The origin of this lies in procuring material after calling for bids against a tender document. The bids are sent to a server which will allow authorized persons to subsequently download and view the same. While the bids are in some standard format, the bid itself must be secured in several ways:

1. The bid document is digitally signed to authenticate its origin and that it has not been altered,
2. It is kept confidential but may be viewed by a set of authorized persons, but only after a certain time $> t_2$,
3. The bid is received before time $< t_1$.

Relevant questions in this case are:

1. How does one ensure that information is not altered during communication and storage within server?
2. In what way are digital signatures relevant?
3. Would access to "public-key certificate" issued by a certification authority be an issue?

Project 5: This project has to do with verifying a document such as a "driver's license" (and this holds good for any "identity card" or for that any official document such as a passport or birth certificate). Typically a police officer looks at the physical driver's license card and simply goes by the information that the license was issued by the "transport authority". Given that it is not so difficult to copy, alter or produce afresh a plastic card, how can one use technology to verify on the go the veracity of a driver license card, when shown to a police officer on the road or elsewhere. (Recall: today cellular based access to Internet-connected servers from smart cell phones is readily available, almost all parts of India.) Questions:

1. How does one ensure that information is not altered during the 2-way communication?
2. In what way are digital signatures relevant?
3. Would access to "public-key certificate" issued by a certification authority be an issue?