TD 6 - Zero-knowledge protocol

The Guillou-Quisquater authentication protocol is the following one. A trusted third part (TTP), issuer of smart cards, has a public key (n, v). The integer n is the product of two large primes p and q; it is assumed that factorization of n is intractable. The integer $2 \leq v \leq n/2$ is chosen such that extracting v-root mod n is considered intractable.
For her public key, Alice uses the public information of her card, that corresponds to a string of characters (for instance, name of the issuer || card number || validity date || ...); this string is a sequence of bits that correspond to an integer $J \pmod{n}$.
The private key of Alice is an integer B such that $J.B^v = 1 \mod n$.
The authentication protocol involves the 3 folowing communications:

1. Alice chooses at random $r \in \{1, \ldots, n-1\}$, computes $T = r^v \mod n$ and sends T to Bob.
2. Bob chooses at random $d \in \{0, \ldots, v-1\}$ and sends d to Alice.
3. Alice computes $D = r.B^d \mod n$ and sends D to Bob.

To authenticate Alice, Bob computes $T' = D^v.J^d \mod n$. If $T' = T$ then Alice is authenticated; else she is rejected.

1. Prove that authentication is correct (soundness and completeness).
Completeness: *if Alice, who knows B, answers correctly, then we have;* $T' = D^v.J^d \mod n = (r.B^d)^v.J^d \mod n = r^v.(B^v.J)^d \mod n = r^v \mod n = T$.
Soundness: *if Eve, who doesn't know B, is correctly authenticated by Bob, then she has sent a correct couple (T, D) to Bob, with D v-root of $T.J^{-d} \mod n$. But she cannot compute v-root; thus the only way for Eve is to compute a couple $(T,\ D)$ verifying $T = D^v.J^d$, then such that $J^d = D^v.T \mod n$, also $D^v.T = B^{-vd} \mod n$. This may be possible for some values of d, for $d = 0$ for instance. But she does not know d; her only possibility is thus to bet on the value of d before sending T: she bets on d, chooses D and computes $T = D^v.J^d \mod n$. Her probability of success in correclty guessing d is only $\frac{1}{v} \leq \frac{1}{2}$.*

2. *We assume that $r^v \mod n$ gives no knowledge on r. Argue that this authentication is a zero-knowledge protocol.*
For any value of d, we have to proove that the transcript $(T = r^v \mod n; d; D = rB^d \mod n)$ gives no information on the secret key B.

- if $d = 0$: we have $D = r \mod n$ and $T = r^v \mod n$. So there is no information on B.
- id $d = 1$: $T = r^v$ and $D = rB$: due to assumption, T gives no knowledge on r; then knowing $rB \mod n$ gives no information on B.
- if $d \geq 2$: Let $B' = B^d \mod n$. We have $T = r^v \mod n$ and $D = r.B'$; similarly to previous case, we have no information on B' except it is a v-power $\mod n$. But if we know B then we know B' by polynomial computation; so, by contradiction, if we do not know B', we do not know B.

3. Previous protocol is extended as follows in order to provide Alice a protocol to sign any message M.

1. Alice computes $T = r^v \mod n$ with r chosen at random.
2. Alice computes $d = H(M||T)$ where H is a hash function on $\log_2 v$ bits resistant to collisions.
3. Alice computes $D = r.B^d \mod n$.
4. The signed message is $(M; \sigma)$ where $\sigma = (d||D||J)$ is the signature of M by Alice.

How Bob will verify the signature?
Bob takes the first $\log_2 v$ *bits of* σ *and computes* $T' = D^v J^d \mod n$. *Then it computes* $d' = h(M|| \; T')$. *The signature is verified iff* $d = d'$.